C.1 BACKGROUND

The Defense Manpower Data Center (DMDC) supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security, and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970s, covering all Uniformed Services, all components of the Total Force (Active Duty, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data for the Uniformed Services. This data supports decision making by the Office of the Undersecretary Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD. DMDC's programs include verifying military entitlements and benefits (e.g., health care, dental, education, and life insurance); managing the DoD Identification (ID) card issuance program; providing identity management for the DoD; employee and Service member travel assistance; personnel and property identification; authentication and access control systems; security clearance, adjudication, and continuous monitoring tools; debt protection for deployed Service members and predatory lending protection for members and their families; personnel evacuation support systems; and assisting military members and their spouses with transition to civilian life. Supporting applications and databases are available to the user community 24 hours per day, seven days per week, with sub-second response time. Any outage can result in disruption of services to DoD beneficiaries as well as potential financial claims from the TRICARE contractors. Additional information about DMDC can be obtained at https://www.dmdc.osd.mil.

This TO will directly support the DMDC Information Technology (IT) Operations (ITOPS) division. ITOPS serves as the DMDC IT Director's agent for implementation and sustainment of information systems and infrastructure used to accomplish DMDC's mission. The DMDC ITOPS division provides IT service management support for information systems located at DMDC enterprise sites, DoD data centers, and Government-Furnished Equipment (GFE) located at off-site facilities.

C.1.1 PURPOSE

DMDC requires IT support services and solutions that span the entire spectrum of existing and future technical environments, hardware and software systems, and lifecycle applications in support of both its unclassified Non-secure Internet Protocol Router Network (NIPRNET) and classified Secure Internet Protocol Router Network (SIPRNET) environments. DMDC is seeking to consolidate its legacy applications currently residing in multiple data centers on SIPRNET and NIPRNET environments, by migrating these applications to a primary and failover site, while maintaining high-level network availability, secure operations, and quality customer support.

C.1.2 AGENCY MISSION

DMDC's mission is to collate personnel, manpower, training, financial, and other data for the DoD. DMDC collects and maintains an archive of automated manpower, personnel, training, and other databases for the DoD. This agency supports the information requirements of the OUSD for P&R and other members of the DoD manpower, personnel, and training communities with accurate, timely, and consistent data. The actions of DMDC ensure that DoD can operate DoD-wide personnel programs and conduct research and analysis as directed by the OUSD P&R.

The Mission of ITOPS is to collaborate with and provide support to the DMDC stakeholders in order to meet the organizational mission of serving those who serve our country and their families members. ITOPS vision is to become an industry standard organization that provides seamless, unified IT services across the DMDC enterprise through the delivery and sustainment of state-of–the-art technology.

C.2 SCOPE

The scope of this effort is to provide a full range of IT-related services and technical solutions that encompass enterprise-level system administration services, property accountability, asset management, operations, configuration management, change management, incident management, knowledge management, project management, problem management, release management, security management, testing, quality assurance, and sustainment requirements of the DMDC IT infrastructure, as well as infrastructure design and deployment of new system initiatives. This scope also includes the migration of DMDC's applications into a single Development Testing (DEV/TEST), production, and COOP environment structured as a Software Designated Data Center (SDDC) (i.e., private cloud).

Lastly, the contractor shall remain abreast of emerging technologies in the marketplace and recommend changes, modifications, upgrades, and industry best practices. Support shall be provided at DMDC's West Coast Government Office in Seaside, California (CA), secondary sites, and field offices and for remote users across locations identified in Section F.2. Long-distance travel may be required to provide temporary support for all locations.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

DMDC is a geographically dispersed organization with both contractor and Government facilities located in Seaside, CA, Columbus, Ohio (OH), Colorado Springs, Colorado (CO), Fort Knox, Kentucky (KY), San Antonio, Texas (TX), Ogden, Utah (UT), and the National Capitol Region (NCR). DMDC also supports a large remote workforce scattered across the United States (U.S.) The Director of DMDC is located at the Mark Center in Alexandria, VA.

Currently, the DMDC IT environment is comprised of various Defense Information System Agency (DISA), DMDC, and commercial-hosted data centers throughout CONUS, providing operational and research support to over 35 million customers worldwide. DMDC handles approximately 10,000 data requests per year and approximately five million data transactions per day. DMDC's Seaside and Columbus data centers currently host approximately 400 Government-developed applications; this number is expected to increase to 500 or more post application migration. The DMDC helpdesk fields approximately 60,000 software/hardware and security-related calls per year. These applications support critical personnel data as discussed above, and core applications must maintain a minimum uptime of 99.5 percent. This uptime requirement is exclusive of scheduled maintenance windows. Core applications include, but are not limited to, Defense Enrollment Eligibility Reporting System (DEERS), Real-time Automated Personnel Identification System (RAPIDS), Military Lending Act (MLA), Service members Civil Relief Act (SCRA), DoD Self-Service Logon (DS Logon), Fourth Estate Manpower

Tracking System (FMTS), Synchronized Pre-Deployment and Operational Tracker (SPOT) and many more.

Information concerning the current DMDC IT/Network Environment has been provided as a part of the DMDC Enterprise Management Information Technology Services (EMITS) Reading Room.

C.4 OBJECTIVE

The objective of the EMITS effort is to deliver highly secure and effective IT services and cutting-edge technologies that support the operations and advancement of the DMDC mission. Inherent to this objective is the task of creating a more collaborative, integrated, transparent, predictable, and measurable organization. Additionally, the EMITS effort will lead the IT enterprise as a change agent for adopting best practices in governance and information sharing. The end result of these efforts will enable DMDC to provide a highly functioning IT service management solution for its customers and seamless user experience across its portfolio of applications. This TO will assist DMDC with the task of foreseeing the needs of its IT customers, making informed enterprise IT decisions and investments, and rapidly responding to mission priorities. Specifically this order will support the migration and consolidation of over 500 applications into a software-defined data center that provides world-class user experiences, unparalleled security, and high availability across all applications.

C.5 TASKS

Task 1: Program Management

Task 2: Transition Support

Task 3: Policy, Procedures, and Operations Support

Task 4: IT Core Services Support

Task 5: Customer Services Support

Task 6: Transformational IT Support

Task 7: Application Migration Support

Task 8: Surge Support

C.5.1 TASK 1 – PROGRAM MANAGEMENT

Program Management includes the effective and efficient management of all contractor work including the accountability and security of all personnel. Program Management ensures that contractor performance is within agreed upon quality, cost, and schedule objectives. Program Management ensures cost-effective acquisition of IT hardware, software, and services. Program Management also supports Government planning and decision processes with cost estimates, technical plans, status reports, performance estimates, and other decision support information.

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a TO Program Manager (TOPM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DMDC via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/ (Section F, Deliverable 1).

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 3). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the divisions, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR) and Contracting Officer (CO).

At least one day prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 2) for review and approval by the FEDSIM COR and the DMDC Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Draft Project Management Plan (PMP) (Section F, Deliverable 8) and discussion including schedule, tasks, etc.
c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
d. Staffing Plan and status.
e. Updated Transition-In Plan and discussion.
f. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
g. Invoicing considerations.

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide Kick-Off Meeting Minutes (Section F, Deliverable 4) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section F, Deliverable 5). The contractor may develop a format to be approved by the Government. The MSR shall include the following:

a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required for the contractor to execute specific tasks. Net results of Government action or inaction.
e. Schedule (show major tasks and projects, milestones, and deliverables; planned and actual start and completion dates for each).
f. Projected travel for the following six months.
g. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
h. Accumulated invoiced cost and incurred cost for each Contract Line Item Number (CLIN) up to the previous month.
i. Projected cost of each CLIN for the current month.
j. Projected internal training for the following six months.
k. Provide a monthly report of all maintenance warranty and license agreements pertaining to DMDC IT HW/SW as part of the MSR (as referenced in Section C.5.3.1a). This report shall provide early notification prior to required action in the areas of maintenance, warranty, or license agreements NLT 100 calendar days from expiration or required action.

C.5.1.4 SUBTASK 4 – CONVENE AND SUPPORT TECHNICAL STATUS MEETINGS

The contractor TOPM shall convene a monthly Technical Status Meeting onsite at DMDC Seaside with the DMDC TPOC, FEDSIM COR, and other Government stakeholders attending via Video Teleconference (VTC) or teleconference (Section F, Deliverable 6). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting (Section F, Deliverable 7).

Additionally, the contractor shall convene an After Action Meeting (Section F, Deliverable 11) following major outages and issues (i.e., Priority 1) that occur during performance of the TO. The meeting shall include the contractor's Subject Matter Experts (SMEs) and appropriate Government personnel (DMDC TPOC, FEDSIM COR, etc.). The purpose of the meeting is to discuss the information provided in the After Action Report (AAR) (Section F, Deliverable 12) and lessons learned. The contractor shall determine available meeting locations, establish teleconference bridges, and develop agenda and meeting minutes. The contractor shall also capture and document action items, resolutions, and decisions identified during meetings. As part of the meeting, the contractor shall facilitate, capture, and document project lessons learned.

C.5.1.5 SUBTASK 5 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)/INTEGRATED MASTER SCHEDULE (IMS)

The contractor shall document all support requirements in a PMP/IMS (Section F, Deliverable 9). The contractor shall provide the Government with a draft PMP/IMS (Section F, Deliverable 8) on which the Government will make comments. The final PMP/IMS shall incorporate the Government's comments.

The PMP/IMS shall:

a. Describe the proposed management approach.
b. Include milestones, tasks, and subtasks required in this TO.
c. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
d. Describe in detail the contractor's approach to risk management under this TO.
e. Describe in detail the contractor's approach to enterprise communications, including processes, procedures, communication approach, and other rules of engagement between the contractor, DMDC divisions, other DMDC contractors providing application development support and security support, and FEDSIM.
f. Contain a decision log to provide a concise, centralized record of all decisions, approvals, or agreements affecting the scope, schedule, or internal and/or external deliverables for the TO.
g. Contain a Communication Plan to identify and track all required communications in support of the PMP, which identifies all key stakeholders and appropriate communications format (meetings, briefings, SharePoint, etc.) content and schedule for each stakeholder.
h. Contain a Quality Control Plan (QCP) to identify the contractor's approach for providing quality control in meeting the requirements of the TO. The contractor's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives.

The PMP/IMS is an evolutionary document that shall be updated annually at a minimum (Section F, Deliverable 10) until such as time as this information is available on the Integrated Operational Dashboard (See Section C.5.3.4) /knowledge management site. The contractor shall work from the latest Government-approved version of the PMP/IMS.

C.5.1.6 SUBTASK 6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (Section F, Deliverable 14, Section J, Attachment G) when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained/benefits.

C.5.1.7 SUBTASK 7 – DMDC IT MATURITY AND OPERATIONAL PROJECT MANAGEMENT SUPPORT

The contractor shall support the IT maturity of the DMDC organization and shall adhere to the policies and processes established by the Government's process improvement initiatives in accordance with industry best practices such as Carnegie-Mellon's Capabilities Maturity Model Integration (CMMI) and Information Technology Infrastructure Library (ITIL). A CMMI evaluation has not been completed, but DMDC's strategic goals include achieving a CMMI Level III certification.

The contractor shall develop an integrated master calendar of all projects and the major milestones for each to provide a high-level executive picture of all project activities (Section F, Deliverable 13). The contractor shall submit the integrated master calendar to the FEDSIM COR and DMDC TPOC after transition is complete and Full Operating Capability (FOC) achieved. The contractor shall maintain a real-time calendar of ongoing projects reflected in an Integrated Operational Dashboard (See Section C.5.3.4). This includes maintaining, refining, and revising the project collaboration sites currently on SharePoint or other Government-designated repositories. This site must include project overview documents, a consistently updated document library that preserves document history, schedules, a dashboard, assignment and POC lists, summaries and agenda for all meetings and conferences attended, and support for collaborative editing/versioning of project documents.

The contractor shall attend a bi-monthly project review meeting to discuss status of all projects and provide updated information regarding the "health" of the high visibility projects. The "health" should include current status, risks, issues, concerns, hurdles, recommendations for improvement, and implementation strategy of recommendations.

C.5.2 TASK 2 – TRANSITION SUPPORT

Transition-In ensures the smooth and orderly transition from the current contract. Transition-Out ensures all knowledge, data, material, and information developed by or provided to the contractor is transitioned and delivered to the Government by the end of the TO.

C.5.2.1 SUBTASK 1 – TRANSITION-IN:

The contractor shall ensure a smooth and orderly 90-day Transition-In period to establish required support. Transition shall begin immediately upon Task Order Award (TOA), and staffing shall be phased in over time as the existing DMDC ITOPS TO expire.

Initial Operational Capability (IOC) shall be achieved no later than two weeks after TOA for the following tasks:

- Section C.5.3.4 NIPRNET IT OPS Integrated Operational Dashboard
- Section C.5.5.2 DMDC Registration Authority (RA) Support
- Section C.5.6.2 Provide Architecture Analysis and Tech. Evaluation Support
- Section C.5.7 Application Migration Support

Full Operational Capability (FOC) shall be achieved 90 calendar days after TOA for the remaining tasks not listed in the bulleted IOC list above. Note: At time of TOA, full responsibility for management and performance for the remaining tasks (i.e. tasks not listed in the bulleted IOC list) will remain with the contractor supporting the existing DMDC ITOPS TO until the end of the 90 day transition period. However, transition activities to ensure a smooth and orderly Transition-In period shall continue until FOC is achieved. IOC is defined as follows:

a. All required staffing to accomplish Transition-In activities are in place.
b. The initial baseline Time-Phased Labor Mix, as specified in Section C.5.2.1, has been submitted to the Government and required staffing in-processing activities are in progress.
c. Coordination efforts are established and synchronized with the existing DMDC ITOPS contractor for their transition out activities (facilitated by Government).
d. The contractor is in full control of transition activities and required DMDC support is being effectively managed.
e. For tasks starting concurrently with TO award, IOC is achieved when items a. through d. above have been accomplished, but no later than two weeks after TO award.

FOC is defined as follows:

a. All tasks are fully staffed with fully qualified and trained personnel.
b. The contractor assumes full responsibility for management of all TO requirements.
c. All TO performance measures are in force and enforced.
d. No further support required from the outgoing contractors.

The contractor shall submit its Initial Transition-In Plan and Time Phase Labor Mix (TPLM) on or before project kick-off for Government approval (Section F, Deliverable 16). The contractor shall submit its Final Transition-In Plan & Time Phase Labor Mix within 10 workday of receipt of Government comments on the Initial Transition-In Plan & Time Phase Labor Mix (Section F, Deliverable 17). The Transition-In Plan shall culminate with FOC achieved 90 calendar days after award and include measurable milestones and decision gates (with entrance and exit criteria) for Government review. The TPLM shall identify all personnel and positions to transition to the TO, when they transfer, and their role. The Government will review and accept this TPLM as the initial baseline.

C.5.2.2 SUBTASK 2 – TRANSITION-OUT:

The contractor shall develop a Transition-Out Plan (Section F, Deliverable 19) for facilitating the accomplishment of a seamless transition and delivering all material and information from this TO to an incoming contractor and/or Government personnel at the expiration of the TO. The Transition-Out Plan shall identify all Government-Furnished Material and Contractor-Furnished Material (GFM/CFM) as well as information and material developed during the TO that was used in the execution of this TO. The Transition-Out Plan shall be submitted for Government approval. Upon incorporation of comments and Government acceptance, the contractor shall follow the Transition-Out Plan to transfer all material, information, and rights thereto to the Government.

The contractor shall provide a Transition-Out Plan NLT 120 calendar days prior to expiration of the TO.

The contractor shall facilitate and conduct transition-out activities. The contractor shall update system descriptions and technical descriptions of all software, systems, and mission-support activities delivered or performed under this TO. The contractor shall support transition of administrative and privileged access to the incoming contractor, ensuring that no administrative access is lost. The contractor shall prepare a final report documenting the status of all ongoing efforts and projects and a smart book/turnover binder containing copies of all plans, policies, procedures, POCs, file storage locations for technical diagrams and documentation, institutional knowledge, and other information requested by the Government. Transition-out shall ensure no disruption to vital Government business. The contractor shall provide full cooperation in providing necessary operational knowledge to the incoming contractor.

Transition-out shall include the following types of services:

a. Project management processes.
b. Identification of POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives and projects.
e. Incumbent contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Identification of schedules and milestones.
h. Identification of actions required of the Government.
i. Establishment and maintenance of effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings.

C.5.3 TASK 3 – POLICY, PROCEDURES, AND OPERATIONS SUPPORT

Policy, procedures, and operations support ensures asset and inventory accountability for DMDC IT, change management activities, portfolio management of DMDC IT portfolio, and Disaster Recovery (DR)/COOP policy and services. The following are the processes, controls, and procedures in order to perform the day-to-day operations of DMDC's network and datacenter. This includes all of the subtasks of asset and property management (with its fiduciary requirements), IT Service Management (ITSM) to include capacity, release, incident, and problem management along with availability.

C.5.3.1 SUBTASK 1 – PROVIDE ASSET MANAGEMENT SUPPORT AND PROPERTY ACCOUNTABILITY

The IT asset management function is the primary point of accountability for the lifecycle management of IT assets throughout the organization. Included in this responsibility are development and maintenance of policies, standards, processes, systems, and measurements that enable the organization to manage the IT Asset Portfolio with respect to risk, cost, control, IT Governance, compliance, and business performance objectives as established by the DMDC.

IT property accountability is the management and tracking of property (hardware and software) upon receipt, delivery, or acceptance throughout the property's useful life and through disposal regardless of the property's status within the property lifecycle (e.g., excess, obsolete or unserviceable, or surplus) or its physical location (e.g., loading dock, in-transit, office, or in an employee's possession) in accordance with DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property." The contractor shall ensure the proper tracking and logging of all hand receipts for remote and mobile devices, according to DMDC, Defense Human Resources Activity (DHRA), and DoD policies, processing receipts and updating applicable property databases to include the DoD Property Accountability System (DPAS).

DMDC asset management is a standard accountancy process concerned with the asset lifecycle from procurement, asset receipt, tracking, maintenance, transfer, and disposal of assets. Assets include hardware, software, consumables, maintenance contracts, and procurements for the DMDC Enterprise. Asset Management function maintains an asset management database which maintains and tracks information such as asset values, asset disposition, current ownership, End of Support Life (EOSL), and location of assets. The role of the DMDC asset management process is the oversight, support, communication and maintenance of the asset management process standard DMDC enterprise wide.

The contractor shall comply with all DMDC and DPAS property accountability activities by ensuring that IT assets are processed through DMDC inventory accountability processes following all applicable DoD accountability processes. The contractor shall update DPAS in accordance with DoD-mandated instructions. For accountable IT assets, the contractor shall report movement, replacement, and disposition to the DMDC hand-receipt holder.

The contractor shall mature an enterprise-wide IT asset management program, which includes the entire asset accountability lifecycle from purchase through disposition with the Defense Reutilization and Marketing Office (DRMO). This task includes maintaining applicable asset management systems, as well as tracking expiration of licenses throughout the system lifecycle by advising the Government of impending expirations in accordance with timelines indicated in this TO. The contractor's program shall track, manage, and coordinate the purchase of new equipment hardware/software, replacements, and upgrades. The contractor shall proactively plan and identify upgrades, updates, and end-of-life planning. The contractor shall process end-of-life, defective, and/or damaged equipment appropriately. The contractor's program shall enable DMDC to effectively manage the lifecycle of its IT assets (i.e., all equipment, hardware, and software within scope of this TO).

The contractor shall assist in the creation and update of DMDC asset management Standard Operation Procedures (SOPs), and maintain current SOPs while ensuring appropriate coordination and approval by the DMDC Government Lead as well as the Division Director. The contractor shall support the publishing and maintenance of policies, process, procedures (Section F, Deliverable 20) and checklists related to the asset management function. Documentation shall be available on the DMDC intranet (SharePoint and/or Service Desk Tool). The contractor shall provide required reports, inventories, and property control procedures.

In support of asset management, the contractor shall:

a. Provide a monthly report of all maintenance warranty and license agreements pertaining to DMDC IT HW/SW as part of the MSR.

b. Provide early notification and coordination with the DMDC TPOC and appropriate resource advisor of maintenance, warranty, or license agreements NLT 100 calendar days from expiration.

c. Monitor and maintain the equipment (hardware and software) asset management license data repository that records and tracks all information pertinent to the lifecycle maintenance of the product (e.g., vendor name, software name and version, number of authorized users and/or devices covered, licensing fees, commencement and expiration date, etc.)

d. Ensure equipment installed on the DMDC enclave networks is licensed, and any software without an available license requires written permission from the Government TPOC.

e. Track and maintain an inventory of all equipment issued to DMDC personnel and forecasting future requirements to include the following consumable items: printer toner, printer replacement parts (such as fusers and drums), CAC readers, projector light bulbs, natural keyboards, specialty mice and trackballs, microphones, and webcams. The report shall also show the previous three month's replacement needs, and recommendations for future purchases of consumable items to ensure a stock is always on hand and readily available to prevent future service outages due to not having available stock.

f. Deliver up-to-date equipment inventory lists and system data to the Government upon request (Section F, Deliverable 23).

g. In support of the Enterprise Services Directorate, the contractor shall implement from a Deployable Technology List (DTL), coordinating with the ITOPS division; ITOPS provides input to server Operating System (OS) versions, and is responsible for the enforcement of deployable technologies. The DTL provides a listing of all approved software for use within the DMDC enterprise.

h. Coordinate licensing, maintenance renewals, and warranty repairs with third-party vendors. This includes coordination for new releases as well as market research for maintenance renewals.

i. Maintain all non-mobile-based IT equipment inventory and functionality, including network printers, copiers, and VTC components that are located in conference rooms and hoteling spaces, as required.

j. Maintain the DMDC web-accessible information store of IT asset data (hardware and software data) repository to be referred to as the Configuration Management Database (CMDB) or equivalent. DMDC currently uses ChangeGear as the ticketing system. The contractor shall integrate the CMDB Tracking System with incident/problem tickets, change order tickets, and configuration and knowledge management documents. The inventory catalog shall accurately reflect asset data for all IT assets in the DMDC enterprise in the NIPRNET and SIPRNET environments.

k. The contractor shall perform an initial IT asset (HW/SW) inventory within 90 calendar days of TO award (Section F, Deliverable 21). The contractor shall also perform an annual inventory of all physical IT equipment, Commercial Off-the-Shelf (COTS) software, and expendable stockage, updating the CMDB (or equivalent). The contractor shall provide a report 30 calendar days after the completion of initial inventory and every year thereafter in the form of an annual inventory report. The annual inventory report shall address the accuracy of the inventory, types of issues encountered, corrective actions, and dates in which the corrective actions are to be completed to ensure ongoing maintenance of the CMDB. This task includes obtaining physical inventory of all locations. When DMDC's assumes responsibility for new IT assets, the contractor shall perform an inventory of these assets within 90 calendar days (Section F, Deliverable 24).

l. Perform reviews as requested by the Government of software license counts by version ensuring non-overuse of utilized software. The contractor shall maintain continuous maintenance contract status via the contractor-created Dashboard (See Section C.5.3.4). The contractor shall make available on the dashboard a report for software license and version count usage issues and maintenance support contract disposition to allow the Government to ensure software contract continuity. The contractor shall notify the Government upon release of an updated version of software on DMDC's DTL, as well as the unsupported date of the current version(s) that DMDC is using so the Government can work with the contractor to develop a migration path to update to the newer version.

m. Ensure maintenance coverage on IT assets (hardware and software), advising the Government within six months minimally ahead of equipment nearing End-of-Lifecycle (Section F, Deliverable 25).

n. Notify the Government not less than 12 months prior to the date on which software/hardware becomes unsupported or decommissioned by the manufacturer. In the event that a vendor announces the withdrawal of support or decommission of a product less than 12 months in advance, the contractor shall notify the Government as soon as possible, but NLT 15 calendar days from the date of the announcement (Section F, Deliverable 26).

In support of property management, the contractor shall:

a. Provide support for the shipping and receipt of equipment. All equipment shall be shipped to a Government site and signed off on by a Government POC.

b. Notify the Government POC's quarterly when excess to DRMO is required. All government property must follow the DoD disposal process. Prior to the disposal of unserviceable items, disposition instructions must be provided by the Government POC.

c. Support DRMO procedures at DMDC in accordance with National Institute for Standards and Technologies (NIST) guidelines (NIST Special Publication 800-88, Revision 1). The contractor shall identify and prepare EOSL equipment within two weeks of removal from inventory. Additionally, the contractor shall prepare IT assets for disposal and shipment by sanitizing and excessing assets in accordance with the DRMO policy. The contractor shall notify the Government POCs (IT Operations, Human Resources, and Facilities) quarterly when excess to DRMO is required. The contractor shall support DRMO activities no less than quarterly and submit quarterly DRMO reports (Section F, Deliverable 27). The contractor shall support updates to the asset management repository and DPAS.

d. Ensure all IT equipment is properly bar-coded and given security classification labels entered into the inventory management system within five workdays after receipt. Once bar coded, the IT equipment shall be entered into the property management system

(DPAS) and added to the DMDC inventory management tool once the inventory is added to the network. The contractor shall perform monthly reconciliation of all receipts and transfers of inventory.

e. Ensure all IT equipment status changes are properly documented in the asset management system NLT five workdays after the date of change and post monthly reconciliation reviews. Once assigned an Internet Protocol (IP) address, the IT equipment shall be entered into the DMDC asset management tool once the inventory is added to the network.

C.5.3.2 SUBTASK 2 – PROVIDE IT SERVICES TO THE DMDC ENTERPRISE

DMDC ITSM is concerned with delivering and supporting IT services that are appropriate to the business requirements of DMDC. IT service quality is maintained and improved through a constant cycle of reviewing, monitoring, and reporting to meet the customer’s business objectives. The DMDC ITOPS division maintains documented IT service offerings, delivers documents, and provides future planned IT services offerings. DMDC averages approximately 10-20 projects per month that support DMDC’s strategic to operational initiatives, cyber directives and other requirements. IT requests will follow the DMDC and Operations Management Project Request processes and will go through a formal DMDC governance review process.

In support of application portfolio management and communication, the contractor shall facilitate the stakeholder engagement sessions to establish stakeholder registers, collaborative sessions, and assist in advancement of organizational maturity in IT services. The contractor shall utilize best practices in the area of portfolio management proposing innovative tools to formalize processes. The contractor shall collect and establish a repository of stakeholder issues, risks, and concerns and store in the contractor-provided Operational Dashboard (Non-Secure Internet Protocol Router (NIPR) only) (Section F, Deliverable 28).

The contractor shall analyze the project portfolio at least quarterly to determine the optimal mix and sequencing of interrelated project requirements and activities to achieve the most effective and efficient consolidated use of resources, cost, labor, infrastructure, and technology.

In support of IT services, the contractor shall:

a. Develop and maintain an internal online IT service catalog, as defined in Section 9.1.6, “Service Catalog Management (SCM),” of the DoD Enterprise Service Management Framework (DESMF), Edition III, March 4, 2016, and support the development of a model to assist the Government in selecting services and management in developing detailed business cases and cost models for calculating the cost of IT services. The catalog shall identify the IT services along with the definition/description, category, and dependencies (Section F, Deliverable 29).

b. Perform an annual analysis of the service level management and provide a report which identifies and recommends applications for rationalization, consolidation, lifecycle replacement, etc. The contractor shall continuously review the portfolio of IT services for applicability and demand (Section F, Deliverable 30).

c. Facilitate and support projects and governance boards (e.g., Architecture Review Boards (ARBs), Change Configuration Boards (CCBs), Change Management, Cyber Security meetings, and other technical meetings and boards as directed), including the review of projects entering the execution pipeline, reviewing the forecast of upcoming releases, and leading discussions regarding schedule, conflict, and resolutions.

d. Support internal and external audits, inspections, Red Teams, etc. The contractor shall assist the Government in aligning projects with organizational priorities and capabilities. These reviews include Financial Improvement Audit Readiness (FIAR), Federal Information Systems Controls Audit Manual (FISCAM), Statement on Standards for Attestation Engagements (SSAE), Cyber Protection Teams (CPT), and other audits.
e. Assess the underlying IT environment within the organization making recommendations on how to achieve long-term scalability, reduce operational cost, and better support business processes.
f. Provide and update an annual Technical Refresh Plan (TRP) (Section F, Deliverable 31) based on the infrastructure service provider to support programmatic growth to include addressing user expansion and technology refreshment planning for all hardware, software, and middleware used. The TRP shall include a methodology that determines the best approach and timing for design refreshment and the optimum mixture of actions to take at those design refreshes as needed.

C.5.3.2.1 SUBTASK 2.1 – PROVIDE INCIDENT AND PROBLEM MANAGEMENT

DMDC incident (unplanned) management goal is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. The goal of problem management is to minimize the adverse impact of incidents, within the IT Infrastructure, and prevent the recurrence of incidents related to these errors by investigating and proposing root cause corrections. At DMDC, incident management is accomplished through a partnership with the Consolidated Contact Center (CCC). Note: CCC support is outside the scope of this effort. CCC fields calls from external end users 24 hours and 7 days a week (24x7). The CCC has the responsibility for fielding calls from external end users and providing the central meet-me-line for incident coordination. The CCC will also contact any additional technical experts required to support resolution of the incident, as requested by the incident manager.

The contractor shall establish a virtual Network Operations Center (NOC) which will include staffing to continuously monitor supporting infrastructure and capabilities for emerging and actual incidents, problems, concurrent outages, and other events impacting IT performance and/or cybersecurity status. This support shall include subject matter experience to respond on a 24x7x365 basis to incidents impacting service availability. The goal of the NOC is to identify potential problems and take action for resolution before they become incidents, whenever possible.

The contractor shall support incident and problem management processes by providing proactive, continuous monitoring of infrastructure capabilities and performance. The contractor shall ensure proper investigation of identified problems and respond to all service outages to include the following:

a. System administration.
b. Network.
c. Telecommunications.
d. Virtual administration.

e. Web middleware administration.
f. Database administration.
g. Storage Area Network (SAN) administration.
h. Cluster Management, etc.

The contractor shall maintain the ability to provide support on a 24x7x365 basis at the declaration of an incident and must be engaged through service restoration. The contractor shall take a proactive approach to capacity management, ensuring integration with the capacity management team for any trends and ensuring space and capacity do not become an incident. The contractor shall coordinate with the application stakeholders to determine the proper event threshold levels.

The contractor shall manage, identify/classify, record, correlate, and categorize AARs (Section F, Deliverable 12) as required by the Government. The contractor shall assign and track corrective and preventative action items until resolution. The contractor shall work across DMDC divisions, contract partners, and external organizations to ensure production outages are resolved timely.

The contractor shall restore normal operation after an incident, prepare root cause analysis, and apply ITIL best practices ensuring business impact is minimized and no further production outages occur.

Additionally, the contractor shall perform the following tasks:

a. Schedule all planned downtime as to minimize impact to users and communicate planned events and expected restoration time to affected users no less than two workdays before the event.
b. The incident manager shall respond to production outages within 10 minutes of identification and notification by the CCC.
c. The supporting technical expert (network, server, etc.) shall respond within 30 minutes of notification by the CCC.
d. Coordinate with ITOPS teams and/or cross divisional groups, external organization, and/or contract partners to isolate/identify/resolve incidents.
e. Provide stakeholders with updates in accordance with the application severity outage in the event of an incident or a planned outage which lasts longer than the originally scheduled event.
f. Upon receipt of system failure/incident notification, treat the incident as severity level 1 until identified otherwise. The contractor shall provide support to the service outage to coordinate and triage troubleshooting efforts through successful service restoration.
g. Categorize and correlate incidents to trigger the corrective action and/or escalation.
h. Maintain an incident and problem management program in accordance with DMDC SOPs.
i. Document the incident from start to finish in order to build a knowledge base to update checklists, SOPs, and lessons learned for each production environment.
j. Create a ticket and categorize and conduct an initial diagnosis of incidents. The contractor shall provide a near-real-time status of all IT incidents and coordinate with problem management on cause, resolution, and prevention of incidents.

k. Apply corrective actions and establish workarounds during incident management to restore service. Document errors and workarounds when identified during incident management/problem management and make available in a knowledge base (i.e., SharePoint and/or Service Desk Tool).

l. As required, contact the support vendor to open a support ticket, creating the appropriate DMDC internal incident ticket with the vendor ticket referenced. The contractor shall provide vendor updates every hour on status.

m. Provide an AAR (Section F, Deliverable 12) for all major incidents within five calendar days of incident closure (Government may request the report sooner depending on the severity of the outage). The information in the report should be based on similar outages, discussions with SMEs, and review of documentation. The contractor shall include in the report a narrative of the outage, meeting discussion notes, action items/assignments, root cause analysis, recommendations, and preventative actions. The contractor shall prepare trend analysis, target preventative actions, and track actions until resolved.

n. Improve efficiency and effectiveness by early identification and addressing root causes of technical problems including working with specialized entities for resolution before they become trends.

o. Develop and maintain an event and issue log to monitor open items until the Government approves resolution and closure (Section F, Deliverable 32).

C.5.3.2.2 SUBTASK 2.2 – PROVIDE CAPACITY MANAGEMENT SUPPORT

DMDC capacity management ensures that cost-justifiable IT capacity for all areas of IT is matched to the current and future needs of the business. Capacity management is a process that extends across the service lifecycle, and it is considered during the service design stage. DMDC capacity management considers all resources required to deliver the IT service and plans for short, medium, and long-term DMDC business requirements.

The capacity management team works closely with the other DMDC ITIL functions to ensure exhausted capacity does not result in an incident. The contractor shall maintain a fully functional Capacity Management Program to include the following activities:

a. Capacity planning and analysis.

b. Measured performance results.

c. Performance management and analysis and reports.

d. Proactive modeling and forecasting.

e. New application and major upgrade sizing formalized measurement.

f. Validate scalability to support future capacity forecasts.

The contractor shall ensure that all current and future capacity and performance aspects of the business requirement are provided by using ITIL practices, standardized methods, and processes. The contractor shall measure process compliance Key Performance Indicators (KPIs), monthly/quarterly reporting) and escalate exceptions to the Government. The contractor shall produce and maintain specific subject matter for reporting and capacity plan development (processor, memory, space allocation, storage requirements, proposals for configuration changes, etc.).

The contractor shall perform capacity workload planning, reporting and availability analysis for a variety of applications and components and develop and execute capacity projection plans. The contractor shall ensure resource requirements are met, reported on, and communicated to product owners and management teams.

Additionally, in support of capacity management, the contractor shall:

a. Allocate storage space, plan for future projects or acquisitions, review hardware and software configurations, and make suggestions for appropriate storage or backup models.
b. Maintain storage devices, provide analysis of capacity, and provide monthly capacity reports, which forecast at least four months in advance, for the storage device, system, or component. The contractor's four-month capacity forecasts will take into account planned project growth, decommissioning, and new project starts, provide service management processes and show metrics to demonstrate system performance health(Section F, Deliverable 33).
c. Maintain servers, server appliances, SAN, fabric, routers, network switches, firewalls, load balancers, storage devices, provide analysis of capacity, and provide monthly capacity reports for those devices, systems, or components.
d. Provide data center and infrastructure capacity management processes that avoid capacity-related service disruptions, alert the Government via email notification when established performance threshold are within 20 percent of maximum capacity, and determine underutilized resources that may be candidates for consolidation or elimination.
e. Monitor daily performance and quality of service and report on efficiency and effectiveness of the capacity management process. Capacity management shall protect services from capacity-related incidents and service downtime and minimize capacity-related incidents/problems by proactively monitoring. The contractor shall alert the Government via email of any non-urgent anticipated incidents/problems with recommended resolutions. The contractor shall alert the Government via face-to-face or phone of any urgent incidents/problems with recommended solutions.
f. Maintain a performance reports database utilizing automated methodologies for performance planning
g. Gather historical performance data and business driver data and assesses whether systems are performing according to production standards and thresholds set by the capacity planning team.

C.5.3.2.3 SUBTASK 2.3 – MANAGE AVAILABILITY

DMDC Availability Management optimizes the capacity of the IT infrastructure, services, and supporting organization to deliver a cost-effective and sustained level of availability that enables DMDC ITOPS to satisfy its business objectives. DMDC Availability Management covers the design, implementation, measurement, and management of IT infrastructure availability.

The contractor shall produce and maintain an Availability Plan that reflects the current 99.5 percent availability and future (i.e. post application migration) 99.99 percent availability needs of the business. The contractor shall monitor, report, analyze, and review service availability. The contractor shall assess and manage risk by implementing preemptive and corrective countermeasures to ensure availability. The contractor shall make recommendations to the Government on how to improve an application's availability upon request of the Government. (Section F, Deliverable 34)

The contractor shall:

a. Facilitate weekly short-term planning meetings to communicate methodologies to effectively manage events such as maintenance, patching, etc.
b. Establish a comprehensive, proactive, ITIL-based Availability Program.
c. Establish and implement a documented outage management process that is used to plan, schedule, execute, monitor, and document outage activities.
d. Communicate planned outages in a manner that will allow customers to understand the impact to their area. The contractor shall ensure outages have been properly coordinated and approved by customers prior to implementation. Multiple reminder notices shall be sent as outage period approaches.
e. Execute approved maintenance actions in accordance with approved timeframes.
f. Maintain and update the configuration management database of assigned systems, their input requirements, and their impacts of service disruptions for use in the service restoration process.
g. Maintain and publish (on the DMDC intranet) a daily outage schedule for assigned systems. Update schedule as changes occur (Section F, Deliverable 35).

C.5.3.2.4 SUBTASK 2.4 – PROVIDE CHANGE MANAGEMENT AND RELEASE MANAGEMENT SUPPORT

DMDC change and release management ensures standardized methods and procedures are used for efficient and prompt handling of all changes to minimize the impact of change-related incidents and improve day-to-day operations.

DMDC release management takes a holistic view of a change to an IT service and should ensure that all aspects of a release, both technical and non-technical, are considered together, thereby reducing potential production outages.

DMDC change management is the ITSM process responsible for all changes. The purpose of change management is to control the lifecycle of all changes - ensuring that all changes to Configuration Items (CIs) are recorded.

C.5.3.2.4.1 SUBTASK 2.4.1 – CHANGE MANAGEMENT

The contractor shall maintain and improve the existing Change Management Program. The contractor shall ensure integration with the DMDC service management community to provide standardized end-to-end support and act as primary focal point for all changes within the DMDC infrastructure, while providing ongoing development and maturation of the change control processes.

The contractor shall provide measurable improvement of Critical to Quality (CTQ) and Critical Success Factor (CSF) milestones during quarterly review cycles (Section F, Deliverable 35), as measured by positive quarterly trends in the efficiency and CMMI-ITIL Process Maturity rates for change management.

Additionally, in support of change management, and upon approval from the DMDC TPOC and change management team, the contractor shall:

a. Ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented in the CMDB, and reviewed in a controlled manner, as described in DMDC's Change Management Process Handbook.
b. Ensure that CSF and CTQ dependencies are addressed and provided within the DMDC change management system. Examples to include are:
    1. Appropriate classification (Routine, Standard, Emergency, etc.).
    2. Categorization of all changes.
    3. Successful implementation of changes.
    4. On-time implementation of changes.
c. Establish, identify, apply, and implement the following ITIL best practices focusing on the items below within the Change Management Team:
    1. Mandatory Checklists for Commissioning/Decommissioning evolutions.
    2. Proper CI attachments on all Change Requests (CRs) that involve changes to any existing CI.
    3. Proper parent/child attachments and proper incident/problem ticket reference correlation.
    4. Integration of the Change Management Process and Short-Term Planning Meetings in order to streamline scheduling conflicts and ensure adequate post-change test and acceptance. The contractor shall provide a planning calendar to identify potential scheduling conflicts with outage and resources. The calendar should consider scheduled outages identified from change and release management, short-term planning, and other groups. The planning calendar shall be made available via DMDC's intranet or application.
    5. Implement standard established CR templates for common, cyclical, or minor CRs to streamline the formalized process.
    6. Implement high priority (Urgent/Critical/Emergency) changes without compromising quality assurance and system performance.
    7. Develop and implement a process to capture root cause of high priority changes (unplanned and otherwise) and drive down the rate of high priority (emergency/critical/urgent) changes.
    8. Workflow and checkpoint improvements to ensure Change Advisory Board and Technical Review Board/Change Configuration Board (TRB/CCB) functions add quality control value to the Change Control process while keeping stakeholders fully informed.
d. Report Operational Change Management Metrics in accordance with CMMI-ITIL Process maturity rates for change management and KPI criteria. Reviews will require no more than two quarterly review cycles to meet acceptance levels. KPIs should reflect positive monthly and quarterly trends in the accuracy and quality of existing CRs.
e. Review existing change management and track policy and procedures (Section F, Deliverable 36) and update them as needed to address CRs and application defects from

receipt through review, analysis, development, and installation. The contractor shall identify CRs that will materially impact the posture of a Risk Management Framework (RMF) accredited system/program and provide the appropriate document to the Government.

C.5.3.2.4.2 SUBTASK 2.4.2 –RELEASE MANAGEMENT

The contractor shall maintain and improve the existing Release Management Program to include the following activities:

a. Governance framework.
b. Change control process phases.
c. Raising and recording CRs.
d. Assessing and authorizing.
e. Planning and implementation.
f. Post-implementation review, closure, and formalized measurement.
g. Auditing and compliance.

The contractor shall perform release and deployment management functions, ensuring that all scheduled outages will be approved by the Government (e.g., Voice Over Internet Protocol (VOIP), infrastructure). The contractor shall use standardized methods and procedures for efficient and prompt handling of all changes in order to minimize the impact of change-related incidents upon service quality, and consequently, to improve the day-to-day operation.

Additionally, in support of release management, the contractor shall:

a. Prepare, build, and test deployment packages and conduct pilots as necessary to ensure successful change implementation.
b. Develop, maintain, and publish on the DMDC intranet a release calendar of all scheduled changes and application deployments. This shall be updated on the first of every month (Section F, Deliverable 37).
c. Coordinate and facilitate release planning meetings with stakeholders and implementation teams. The contractor shall identify and resolve scheduling conflicts and dependencies and confirm the release calendar.
d. Manage the deployments of changes and applications.
e. Verify and monitor early life of fielding and correct any issues. All deployments shall have a minimal impact on the customer and operations.
f. Ensure back-out plans exist and execute when necessary due to adverse or unanticipated impact of changes or deployments.

C.5.3.2.5 SUBTASK 2.5 – PROVIDE CONFIGURATION MANAGEMENT SUPPORT

Configuration management refers to the discipline of evaluating, coordinating, reviewing, and implementing changes in artifacts (e.g., CIs) that are used to construct and maintain software systems, IT components, and services throughout their lifecycle. CIs are any assets that need to be managed in order to deliver a service. CIs that should be under the control of configuration management include hardware, software, systems, services, applications, their relationships, and associated or related documentation, (e.g., Service Level Agreements (SLAs)). Software configuration management is the task of tracking and controlling changes in software as well as reporting current status and change history of software components (including source code, documentation, problems, changes requested, and changes made). The goal of software configuration management is to establish and maintain the integrity of software components from initial concept through design, implementation, testing, baselining, building, release, and maintenance by ensuring configurations are properly evaluated, authorized, and implemented.

The contractor shall maintain, update, and improve the existing configuration management program to address all new and/or modified hardware, firmware, software and documentation. The contractor's configuration management program shall define the CIs, including establishing and maintaining CI classifications; establishing and documenting the configuration management processes which adheres to the process workflow guidance for configuration management as defined in the DESMF, with a focus to improve the current configuration identification, configuration control, configuration status accounting, configuration verification and Audit; establishing release cycle baselines/documentation, establishing a verification process, and providing for other areas of configuration management governance. The contractor shall utilize automated tool, (e.g., Puppet) where appropriate in order to develop a positive return on investment (ROI). The configuration management program shall be planned, documented, and established with direct coordination and phase approval of the Government. The contractor shall ensure that the configuration documentation for software releases properly aligns with the DMDC environment.

The contractor shall perform configuration management activities of configuration status accounting, configuration baseline management, creating and maintaining a configuration management library system to control the release of products in order to manage their history, and administering a centralized change management procedure and centralized tool to track all CRs or Problem Reports (PRs) to the baseline as well as all issues (PRs). Configuration management scope includes COTS and Government Off-the-Shelf (GOTS) software, database-deployable objects, and hardware. The contractor shall respond to documents delivered with the software release and update and re-deliver documentation if not approved.

The contractor shall design, publish, and implement a plan to transition from legacy configuration management tools to modern scalable industry standard tools including a unified system for hardware and software changes (including COTS) (Section F, Deliverable 38). This system shall contain approval workflows and task routing as well as a graphical user interface to the automated build and deployment scripts (shell scripts, Python, and WebLogic Scripting Tool).

The contractor shall identify, describe, and track software and hardware configuration items and their dependencies. The contractor shall coordinate with the Government prior to any planned configuration changes, outages, or Authorized Service Interruptions (ASIs). The contractor shall institute DMDC-compliant Change Configuration and Release Management (CCRM) processes for the operations and maintenance of the network, documenting all actions using the DMDC Enterprise Problem and Change Management SOP. All changes should be documented in monthly Change Reports (Section F, Deliverable 39).

Additionally, in support of configuration management, the contractor shall:

a. Identify, record, track, and report on all deviations from configuration management standards.

b. Review and grade completed production-level changes for accuracy, completeness, and adherence to process and standards.

c. Perform random auditing to compare the configuration database to the actual deployed version on servers.

d. Resolve configuration audit exceptions.

e. Reduce the number of exceptions reported during configuration reports.

f. Monitor, fine tune, and update the build/deploy automation scripts to incorporate changes in policy or environment.

g. Oversee, build, and deploy automation work, proactively review issues and failures, fix them, resubmit failed attempts, and document issues and fixes.

h. Perform release management functions for DMDC; coordinate software releases among all divisions.

i. Design, implement, and maintain release strategies for the DMDC Common Update Framework.

j. Publish and make available dynamic real-time reports for all (daily, weekly, monthly, and biannual) DMDC production releases to include item name, item version, quality assurance status, current environments deployed to, release date, and dependencies.

k. Provide ad-hoc self-service reporting capability for DMDC authorized users on CI status.

l. Support Software Request for Change Approval Process (SharePoint workflow and InfoPath Forms) - manage the "Request for Change" workflow which runs on SharePoint using InfoPath forms.

m. Support Source Control software management and account provisioning - manage and maintain the source code repository and repository admin tool.

n. Support the Technical Review Board for software changes by providing technical review of proposed changes for feasibility, timeline, risk, etc. Ensure documented requirements are met for production deployment.

o. Manage DMDC's implementation of its definitive media library. DMDC currently uses Maven but is tool agnostic.

p. Manage and maintain DMDC's Java Deployable Technology List (Java DTL).

q. Manage the Configuration Management Work Queue. The contractor shall assign all tickets to individuals in the time specified by DMDC policy.

r. Triage failed builds and deployments. The contractor shall review build/deployment script logs and server logs to help recognize patterns of failure.

s. Categorize and track failures, work with other teams to identify root causes, and implement fixes.

t. Perform manual deployments to application servers if automation is not working properly.

u. Maintain software web application configuration database which supports automated and manual software web application deployments and application release governance.

v. Provide technical support and assistance that corrects all systems malfunctions; provide maintenance of new and modified systems and applications software to ensure availability, operability, and efficiency.

w. Maintain web application configuration management software that supports automated and manual application deployments and release governance.

x. Provide technical support for the existing build and deployment automation scripts to include subject matter expertise in Python, Perl, Docker, Gitlab, Jenkins, Web Logic Scripting Tool (WLST) and traditional UNIX shell scripting.

y. Analyze the needs and capabilities of the automated build and deployment system, research industry standards, provide recommendations for possible replacement by COTS solutions, and install, manage, and perform the day-to-day functions, including troubleshooting, requirements updates, and general maintenance of the new solution or existing scripts.

z. Make recommendations to the Government on how to improve the configuration management plan in a manner that follows industry standards utilizing DESMF guidance and applies to the hardware, software, and documentation developed, maintained, or operated by the enterprise.

aa. Provide all baseline system documentation that includes system designs, build procedures, requirements documents test procedures, PRs, software code, and system knowledge base and deliver to the Government upon final Government acceptance of the baseline. The contractor shall ensure that IT configuration changes are documented in the configuration management database. The contractor shall ensure that changes are approved and executed is in accordance with DMDC governance practices.

bb. In the configuration management database, document CI dependencies in the between hardware, software, and other IT assets. The contractor shall update relevant configuration management database CI relationships as configuration changes are executed.

cc. Ensure CI attribute required fields are populated for completeness.

dd. Include in the monthly CR the date the change ticket was opened, users affected, nature of any changes, and the status of the implementation of the change.

ee. Evaluate proposed configuration management changes and provide solutions to improve the quality of the change package and/or its likelihood of successful deployment.

ff. Update the deployment calendar quarterly for routine infrastructure software, network, and database upgrades (OS, browsers, databases, web applications, etc.) on SharePoint.

gg. Provide a quarterly status of infrastructure upgrades (completed, on time, behind schedule, delayed, postponed, etc.).

hh. Provide maintenance support for configuration management system GOTS application utilizing Microsoft Access database and Oracle database for policy or ownership changes.

C.5.3.2.6 SUBTASK 2.6 – PROVIDE KNOWLEDGE MANAGEMENT SUPPORT

Knowledge Management (KM) is essential to identification, maintenance, and management of data, information, and knowledge utilized in support of services provided by DMDC ITOPS and the Technical Services Directorate in preparation and support of DMDCs IT service offerings. These offerings include items such as COOP and Emergency Preparedness planning, lessons learned to be included in AAR (Section F, Deliverable 12), transition planning, information security, continuous improvement, project status, tasker tracking, technical requirements, Risk Management Framework (RMF), resource management, and other critical knowledge management artifacts. The contractor shall establish and maintain a KM program to support ITOPS and inform the enterprise and its stakeholders. The KM program will enable collaboration, content management, records management, and business process management. The contractor shall provide standardized structures (taxonomies) for tagging content. The contractor shall provide appropriate individual, role-based access control. The contractor shall store and organize content in a way that it can be efficiently searched.

The contractor shall update an electronic dashboard (See Section 5.3.4) with this information to provide the tracking and display of critical information requirements to efficiently and effectively operate the network and keep stakeholders informed; this includes active management to ensure updates are captured.

The contractor shall provide KM support services that streamline and improve KM processes. The contractor shall facilitate, train, and sustain the ability of KM users to interface with IT operations. The contractor shall improve KM integration with ChangeGear, SharePoint, and other monitoring tools ensuring maximum user access to a self-service knowledge management environment based upon authentication and authorized use.

The contractor shall facilitate the creation and advancement of KM process improvement initiatives such as self-help. The contractor shall also provide documentation and technical writing services that are typical of IT projects and in support of DMDC initiatives (Section F, Deliverable 40); these tasks shall include:

a. Developing and maintaining documentation related to the ITIL processes and/or on-line (website) sources of data.
b. Developing training materials and documentation.
c. Providing analysis based on KM tools to serve as input for changes in SOPs.
d. Developing and maintaining desktop procedures to include the Tactics, Techniques, and Procedures (TTPs) for each support role in this TO (i.e., web administration, desktop support, and active directory administration).
e. Maintain a centralized knowledge-base/repository.

C.5.3.3 SUBTASK 3 – PROVIDE DISASTER RECOVERY (DR) AND CONTINUITY OF OPERATIONS PLAN (COOP)

The contractor shall perform analysis of the DMDC services and maintain, update, and/or develop plans, processes, procedures, and training materials for restoration of operations in the event of an incident or disaster. In accordance with existing DMDC DR and COOP policies and procedures, the contractor shall review and provide input to plans as required, but at least annually (Section F, Deliverable 41). The contractor shall conduct ongoing gap analysis across the DR Program to ensure identification of gaps in planning, documentation, implementation, testing, training, and exercises. The contractor shall take corrective action to remediate any gaps or issues.

The contractor shall provide management of accounts, network rights, and access to systems and equipment; maintain the integrity of system baselines and provide audit checks of all systems and backups as required; and identify and document the functional and physical characteristics of the system CIs, controlling any changes to such characteristics, record and report the change(s) within the Configuration Management Database with the implementation status, and validate conformance to requirements.

The contractor shall provide IT support to COOP and DR efforts and site(s). Long-distance travel to and on-site services at remote sites may also be required to support DMDC DR and COOP emerging requirements.

The contractor shall develop and execute Plans and Procedures (Section F, Deliverable 41), as directed by the Government, for DMDC DR capabilities. These plans will be exercised periodically to ensure that safeguards, backups, end-user services, and procedures can provide continuity of mission support services through issues such as natural disasters, power outages, and building loss and allow successful recovery of all services after facility restoration or the establishment of an alternate facility. COOP and DR planning and exercises must include support for the component's restoration activities.

Additionally, in support of DR and COOP, the contractor shall:

a. Maintain, update, and test the DR Plan for restoration of operations in the event of an incident or disaster on NIPRNET and SIPRNET (Section F, Deliverable 41). Conduct ongoing gap analysis across the DR Program to ensure identification of gaps in planning, documentation, implementation, testing, training, and exercises. Plan shall meet the requirements in NIST 800-84. The contractor shall provide DR Plan 60 calendar days after contract award and provide updates to the DR Plan after application migrations.

b. Maintain and update the business impact analysis, DR, and COOP documentation for DMDC systems. The contractor shall integrate the various aforementioned plans for DMDC as required and dictated by the pace of data center migrations(Section F, Deliverable 42)..

c. Develop system and network designs as a part of the DR Plan that enable business and network operations capable of surviving individual component failure (Section F, Deliverable 41).

d. Provide input to the Government for making system degradation decisions in the event of a disaster or incident; the contractor shall also provide lessons learned following exercises (Section F, Deliverable 43).

e. Execute the service failover COOP requirements and DR plan in the instance of a disaster or emergency.

f. Develop and provide an annual update to support, plan, and execute switchover exercises of the DR Plan (Section F, Deliverable 42).

g. Identify, define, or develop, as necessary, guidelines for off-site storage, replication, physical security, and scrubbing of hardware (cradle to grave) as they relate to all elements of DMDC security.

h. Support the Government's long-term strategy based upon the results and prioritizations of the DMDC mission and strategic plan and the needs of the agency. The contractor shall assist with the development and annual review of Contingency Plan Test Plans to ensure DR requirements are completed and documented, ensuring consistent application throughout the DMDC enterprise.

i. Identify and minimize reliance on resources or entities outside of DMDC control and test DR failover capabilities as directed by the Government. The contractor shall develop contingency test plans, lead tabletop exercises, and assist with gathering IT-related follow-up actions.

j. Exercise both the COOP and DR Plans annually (table-top or actual as directed by the Government). The contractor shall document the outcome of COOP/DR failover test with lessons learned/AARs and provide to Government within 30 calendar days of the exercise (Section F, Deliverable 41).
k. Provide back-up and COOP/DR capability for specified databases, optimize system efficiencies, generate performance reports, and ensure data is only accessed by authorized personnel.
l. Maintain COOP/DR documentation and complete COOP/DR testing as scheduled in the project plan (Section F, Deliverable 42).
m. Update RMF repository with applicable COOP/DR documentation.

C.5.3.4 SUBTASK 4 - DMDC NIPRNET IT OPS INTEGRATED OPERATIONAL DASHBOARD

The contractor shall design, develop, and maintain a dashboard solution that provides program management and operational views, monitors enterprise health, tracks metrics, and reports on a near to real-time basis (Section F, Deliverable 44). The dashboard shall integrate seamlessly and securely with enterprise systems, applications, and data. The objective of the integration is to create automated capabilities that require little to no manual effort. The proposed dashboard solution may leverage existing tools or new technology. The solution shall meet all DoD policies and mandates for system security, including the Authority To Operate (ATO). Over the life of the TO, the contractor shall continually identify opportunities to enhance the dashboard with new integration and capabilities.

The solution shall include the following capabilities:

a. Ability to monitor near to real-time enterprise health and status of systems and services.
b. Integrated views that provide a common operational picture or “single pane of glass.”
c. Operational indicators and updates that provide relevant and actionable intelligence.
d. Near to real-time data collection and metrics.
e. Data analytics.
f. Automated report generation.
g. User-based views (e.g., executive-level, operator-level, etc.).
h. Ability to view the status of the Plan of Action and Milestones (POA&Ms).
i. Blend data from multiple sources into a single view, with drilldowns and interactive intelligence.
j. Perform ad-hoc KPI analysis in real-time.
k. Receive alerts by email or mobile technologies when metrics need attention.

C.5.4 TASK 4 – IT CORE SERVICES SUPPORT

IT core services support includes server maintenance, virtualization, middleware, and database administration support to the DMDC system and infrastructure backbone. This also includes security and patch management compliance, networks and telecommunications support, and support to DMDC's International Business Machines (IBM) mainframe.

C.5.4.1 SUBTASK 1 – PERFORM SERVER ADMINISTRATION (SA)

The contractor shall provide expert subject matter expertise to support system administration of 2,000 plus servers. The contractor shall maintain system configurations and perform operations using privileged accounts on multi-user computer systems (servers). The DMDC system administration staff seeks to ensure that the uptime performance, resources, and security of the servers they manage meet the established uptime performance and capacity requirements of DMDC. The system administration staff installs, upgrades, patches, and remediates computer components and software; provides routine automation; maintains security policies; troubleshoots; trains and/or supervises staff; and offers technical support for projects.

The contractor shall adhere to applicable separation of duties, principle of least privilege, privileged user, two-factor authentication, and role-based access policies and industry best practices.

C.5.4.1.1 SUBTASK 1.1 – SYSTEM ADMINISTRATION

The contractor shall perform administration and maintenance of x86 and Scalable Process Architecture (SPARC)-based computer systems running Windows, RedHat Linux, or Solaris OSs on both the NIPRNET and SIPRNET. The contractor shall document procedures for upgrading and deploying new hardware and software. The contractor shall also test and implement processes for upgrades. All DMDC IT assets must be compliant and host-only supported versions of software and firmware.

The contractor shall provide a wide range of system administration services which may include installing, supporting, and maintaining servers and appliances and planning for and responding to service outages and other problems.

The contractor shall perform system/application diagnostics through the use of tools to ensure availability and to provide notification of problems to the Government.

The contractor shall maintain the integrity of system baselines and provide health checks of all hardware, OSs, and backups. The contractor shall implement COTS applications as applicable and approved by the Government to include scripts and tools.

The contractor shall ensure that any new software to be used within the DMDC environment requires an automated software installation package be created for deployment using DMDC's approved automation tool. Upon approval for use, a software deployment package shall be created and fully tested. Software packages shall be fully tested and available in accordance with the Performance Requirements Summary (PRS).

The contractor shall provide technical support (Tier II) and assistance that corrects all systems malfunctions and maintains new and modified systems and applications software to assure operability, efficiency, and compliance with DoD standards. The contractor shall provide direct support to customers through rapid response to PRs/trouble tickets and respond to requested workload through CRs utilizing ITIL principles.

The contractor shall monitor systems and respond to alerts on Windows, Solaris, and RedHat OSs, SAN, Network Attached Storage (NAS), fiber switches, and blade centers on a 24x7x365 basis, reference virtual NOC requirement. The contractor shall take the necessary actions to address problems using the server incident management process, which includes problem identification, resolution, documentation, and transfer of control among teams, vendors, and other personnel.

The contractor shall perform touch labor on all server/equipment. Locations requiring touch labor are referenced in Section F.2 Places of Performance and the Electronic Reading Room. This shall include such items as tape/disc loading, power up/down (as requested by the customer), maintenance vendor escort, validation of interface connections and status light conditions, cabling, and operations that can only be performed at the physical system.

DMDC currently uses Microsoft SharePoint as its primary documentation repository. DMDC is planning to migrate from hosting SharePoint to a DISA DoD Enterprise Portal Services (DEPS)-hosted instance. The contractor shall provide expertise support to administer DMDC's SharePoint infrastructure, to include development, management, migration, shutdown, and other required support for SharePoint sites, infrastructure, and portals until all are migrated to DISA DEPS. Upon DMDC completion of migration, the contractor shall decommission the DMDC SharePoint server.

Additionally, in support of system administration, the contractor shall:

a. Diagnose software and hardware failures to resolution to maintain high levels of availability.
b. Assist the Cybersecurity Division in the prevention of computer hacking and other security-related problems by implementing preventive measures in compliance with enterprise architecture. The contractor shall ensure all intrusion detection or other information assurance/cybersecurity systems are fully functioning with OSs and are running current revisions.
c. Monitor the performance of the servers/systems and resolve any issues related to their efficient and effective use.
d. Install, support, and maintain a stable, redundant, efficient, and productive computer system and computing environment. These activities include system software maintenance and updates, ensuring compliance with IT security requirements, user account management, configuration management, system upgrade/improvement, computing operations, maintenance of systems documentation and procedures, and contingency planning.
e. Maintain daily, weekly, and monthly scheduled network backups; test and restore data as required to support systems and data recovery due to hardware, software, or user error; verify and validate the integrity of the backups; and perform recovery test or drills quarterly. The contractor shall maintain a log identifying media, date of backup, data contained within backup, and the location of the media. The contractor shall test backups at least quarterly to verify the most recent backup can be properly restored. A weekly backup report shall be provided to the Government (Section F, Deliverable 48)
f. Ensure that current backups are conducted on a daily basis (incremental), with full backups performed on weekends. All other information assurance appliances, systems, networks, and their appropriate IOS/OSs shall be backed up to ensure proper and expedient service restoration in the event of a system outage. The contractor shall provide

a weekly report to ITOPS Management that indicates the status of all backups. Service level for backups and data restoration is 99 percent.

g. Identify and document the functional and physical characteristics of the system (CIs), control any changes to such characteristics, record and report the change(s) within the CMDB with the implementation status, and validate conformance to requirements.

h. Monitor and report on the overall health of the supported servers and applications. The contractor shall provide solutions for application and database issues including capacity, redundancy, replication, and performance tuning.

i. Perform scripting management, automating repetitive processes, and implement version control to ensure effective handling of tasks.

j. Define, develop, manage, and administer processes used to issue and secure user IDs, passwords, and security keys (public/private, unique) in compliance with DoD, DISA, and DMDC standards, policies, and procedures at all DMDC-managed sites.

k. Manage disk space utilization on all servers, including monitoring, and provide a weekly Server Disc Space Utilization Report through a capacity dashboard (Section F, Deliverable 45).

l. Provide access to network shares, directories, files, and SharePoint sites as requested and approved within the helpdesk ticketing system. Verify with end-user owners that access can be provided to the requestor.

m. Define methodology for identifying and managing risks that may affect cost, schedule, and performance; evaluate risk to assess and determine potential outcomes; define steps to respond to and mitigate identified risks; present risk mitigation plan with risks identified; and addresses each risk and changes over time.

n. Maintain a WBS and detailed project plan for all infrastructure projects as a subset of the PMP (Section F, Deliverable 10).

o. Support the physical racking, power-on, and cabling of new or relocated servers to successfully integrate the hardware into the DMDC operational environment.

p. Implement and configure automated tools to detect and monitor the operations of the applications.

q. Perform standard system operation functions and system console operations using DMDC-established processes and procedures. These include:

    1. System reboots.
    2. System stop/start/resets.
    3. Initial system load using the most current OS image (jumpstart/kick-start).
    4. Load/unload of configuration media.
    5. All functions requiring root-level authority.

r. Detect and monitor operations of applications using Solar Winds or other Government-provided monitoring tools. Performance monitoring shall be facilitated with VMWare VROps.

s. Track all incidents from problem identification through problem resolution with the primary focus on immediate service restoration to minimize impact to the user community.

t. Analyze data storage requirements and design appropriate backup strategies, processes, and procedures for all networked systems.

u. Ensure appropriate coordination and flow of information among all necessary parties, including helpdesk support personnel, to quickly restore service availability, minimize service disruptions, and respond to customer needs by using existing incident and service request management tools.

v. Administer OSs security in accordance with published DoD security standards (Security Technical Implementation Guides (STIG), Information Assurance (IA) Vulnerability Management (IAVM), vendor-released patches, higher-level directives and Federal/DoD/DISA policy for vulnerabilities and system patches to ensure server security posture.

w. Ensure current software version and release levels are installed and changes follow DMDC change management processes.

x. Develop and maintain a Standards and Procedures Knowledge Base/Checklist based on best practices for performing system administration, to include storage, middleware, etc. (Section F, Deliverable 20).

y. Monitor and control storage performance according to technical standards and specifications and storage and data management policies and procedures, and perform tuning as required.

z. Request changes to the environment at site and obtain approval from the Government technical team; changes shall originate via a CR.

aa. Provide input to AARs.

bb. Work with the building facilities team to ensure sufficient power and cooling.

cc. Maintain documentation of rack elevations to expedite placement of new equipment.

dd. Execute tasks from Project CRs and associated child CR.

C.5.4.1.2 SUBTASK 1.2 – PROVIDE STORAGE OPERATIONS/FUNCTIONS

The contractor shall manage the disk storage arrays, storage area network, and tape robot systems within DMDC. Responsibilities include developing a storage management program, firmware patching for the entire SAN fabric, arrays and server Host Bust Adaptors (HBA), Logical Unit Number (LUN) layout for SAN, and NAS for all models and makes that are within the DMDC enterprise like NETAPP, HITACHI, HP EVA, SPECTRA LOGIC, BROCADE, PURE and NIMBLE etc. The contractor shall provide employees with an IT1/ADP-level vetting to support the DMDC SAN disk storage configuration management.
Additionally, the contractor shall:

a. Ensure all changes approved through the change management process.

b. Provide problem management support for storage array and fabric.

c. Open a service request with the storage appliance maintenance vendor for error conditions and to ensure proposed configuration/microcode upgrades are vetted by their engineering staff.

d. Execute all volume assignments vetted through the CR process of DMDC storage resources.

e. Maintain DMDC’s storage configuration documentation.

f. Control access to SAN management resources by restricting IDs, passwords, functionality, and IP addresses to individuals directly supporting the resources.

g. Configure and create zones to establish a link between server HBAs and fiber adaptors. Incorporate and maintain the use of a fabric director for the data integrity of the DMDC environment.

h. Provide recommendations for further tuning or optimization.

i. Support, if workload increases or capacity issues exist, the additional capacity required. Supporting this growth and resolving capacity-related issues shall be the responsibility of the storage administrators, in conjunction with Government management.

C.5.4.1.3 SUBTASK 1.3 – SUPPORT CLUSTER MANAGEMENT

The contractor shall manage all of the different types of hardware and software clustering within DMDC's enterprise including, but not limited to, those indicated below. The contractor shall install or uninstall cluster software and configure and administer cluster software packages. The contractor shall also apply cluster software patches, hotfixes, and service packs. The contractor shall maintain Operational Procedures documentation for cluster operations. The types of clustering include, but are not limited to, Symantec Veritas high availability, Oracle Real Application Clusters (RAC), Microsoft Clustering, Virtual Machine Ware (VMWARE) high availability, etc. The contractor shall perform cluster management activities using various cluster technologies. These include, but are not limited to, the following:

a. All aspects of installing/uninstalling the software.

b. Configuration and administration to include startup and shutdown).

c. Applying software patches.

d. Hotfixes and services packs.

e. Maintaining operations procedures documentation.

f. Root cause analysis.

g. Problem resolution activities.

C.5.4.2 SUBTASK 2 – CONDUCT VIRTUALIZATION ADMINISTRATION

The Virtualization Administrator is responsible for the day-to-day operations and maintenance of the Shared Services Virtualization servers and infrastructure. The Virtualization Administrator carries out responsibilities in some or all of the following technical areas: hardware maintenance, system upgrades, infrastructure design and layout, DR design and implementation, hypervisor installation, and maintenance, Site Recovery Manager Deployments, physical to virtual migrations, and hypervisor server hardening.

The contractor shall maintain current industry expert knowledge of development concept, practices, and procedures, and provide subject matter expertise in use of virtual machine (VM). The contractor shall provide subject matter experience in Enterprise Data Centers and demonstrated knowledge and experience with virtualization technologies for Data Center Virtualization, cloud-based computing, and end-user computing (e.g., VMWare, Citrix, etc.).

The contractor shall develop an in-depth understanding of the active virtual IT baseline capabilities, design, and objectives, and provide technical OS documentation. The contractor shall ensure users are trained in applications and OS fundamentals for the entire DMDC virtual infrastructure.

DMDC cloud management intends to build upon the core foundation of virtualization to introduce new abstraction layers through software to increase agility through automation. In addition, the introduction of a self-service multi-tenant model is critical, all the while being fully secure and in compliance (e.g., DISA STIG or DMDC compliance baseline).

Additionally, in support of virtual administration, the contractor shall:

a. Provide for implementation, troubleshooting support, maintenance, and capacity planning of the virtualized computing environment, including day-to-day operations, monitoring and problem resolution for virtual environment issues and problems.

b. Monitor virtualization systems and storage; proactively address or escalate issues before service is impacted; and provide Tier II problem identification, diagnosis, and resolution of problems in the virtual environment.

c. Maintain Operations and Sustainment O&S SOPs for the virtualization environment and diagnose and troubleshoot problems with the virtualization environment, including Microsoft, UNIX, and Linux OS.

d. Support off-hour maintenance activities and support the certification and accreditation process for virtualization hosts.

e. Establish and maintain monthly patching for all virtual systems and evaluate patches before installation utilizing the tool sets provided for the virtual infrastructure.

f. Work with the different business units to develop the engineering design to support the business and operational requirements for either new systems or enhancements to existing systems; interacting with the project engagement teams.

g. Define standard engineering designs, templates, processes, and procedures for implementing projects that follow existing DMDC virtual architectures.

h. Analyze system performance, modifying parameters to improve throughput and effectively utilize system resources. The contractor shall monitor resource usage, making required adjustments utilizing tools like vCenter Operations (vCOPS), vRealize Network Insight, and SolarWinds.

i. Manage all virtual infrastructures (e.g., VMware, Horizon 7 Ent, vCenter, VMWare NSX, vCloud, vRealize, virtual desktop infrastructure (VDI), Citrix, site recovery model (SRM) replication, Oracle logical domains (LDOMS) and zones), hardware virtualization, and infrastructure operations.

j. Manage and support blade chassis and all associated components as it relates to virtual technologies and OS deployments.

k. Participates in on-call production support activities 24x7x365. The contractor shall have the technical knowledge and capability to handle all problems that may arise within a virtual environment. The contractor shall proactively put procedures in place to prevent and reduce the severity of outages and implement automation wherever possible.

l. Architect an industry-standard virtualization layer that includes the following domains: compute, storage, network, operation system, high availability/fault tolerance, DR, and application dependencies which resides in the management domain.

m. Implement VMware vCenter Chargeback Manager (vCBM) to properly bill departments for the resources they utilize.

The contractor shall develop the plan and implement the upgrade, expansion, or replacement of the current DMDC virtual desktop infrastructure.

This plan shall address the following critical factors:

a. Ability to scale in size for future growth of virtual servers and desktops.
b. Centralized management for corporate and personal device options, providing a reduction in hardware and maintenance cost.
c. Migration of 500 users to the new solution within 180 calendar days of completion of infrastructure, to include user data backup and transfer, application readiness, and remote accessibility. By the end of the base period, preparation for the infrastructure to handle migration of the entire population shall be complete.
d. Addresses the requirements for supporting a mobile workforce based on industry standards.

C.5.4.3 SUBTASK 3 – CONDUCT MIDDLEWARE ADMINISTRATION

DMDC maintains a complex web infrastructure with high-availability requirements, supporting internal as well as external end-user and system-to-system interfaces for DMDC’s service offerings. The contractor shall support future web infrastructure component growth as required.

The contractor shall provide the overall administration and maintenance of existing middleware components and the creation of new middleware components and engage in all aspects of middleware administration including architecture, design, configuration, tuning, monitoring, troubleshooting, installation, upgrades, and deployment to various environments. The contractor shall provide technical expertise and support to other staff members on implementing and integrating middleware products and platforms. The contractor shall provide design and implementation plans for all new web or application-specific projects that come to the ITOPS Division. The contractor shall adhere to security and operational parameters and constraints existing at the time the integration is required. The contractor shall administer operation of batch applications.

The contractor shall provide maintenance and sustainment for all existing and creation of new application servers; the application server is a server which provides Java Virtual Machine hosting services to Java 2 Platform, Enterprise Edition (J2EE)-based applications beyond those available from the OS.

The contractor shall serve as the primary escalation point for failed or non-functioning application deployments in the environments provided in the list of COTS products running on the infrastructure (DTL). Currently, there are approximately 400 applications supported with a project growth to reach 500 applications.

Additionally, in support of middleware administration, the contractor shall perform the following:

a. Ensure that middleware infrastructure that supports enterprise applications is scalable and robust to meet current and future provisioning needs. This includes configuring clustered environments as well as DR solutions.

b. Provide proactive monitoring of individual components and the overall middleware products.

c. Develop roadmaps involving middleware technologies to management upon request (Section F, Deliverable 46).

d. Implement and manage effective backup/archive strategies for middleware environments. The contractor shall perform backups, restores, and DR functions including DR drills.

e. Document existing and new middleware platforms and infrastructures with respect to functionality, maintenance, and administration. The contractor shall maintain this documentation in a centrally located place accessible to all relevant team members (Section F, Deliverable 46).

f. Provide support for the administration of web server applications. Administration tasks shall include integration, installation, upgrades, decommissioning, patching, etc. and performing tasks to maximize web service availability and conformance to DMDC and DoD policy.

g. Plan, test, and implement initiatives to incorporate new technologies not currently present within the DMDC web environment.

h. Develop implementation plans for continual availability improvements of web services and submit for Government approval annually, with the initial report 90 calendar days after TO award (Section F, Deliverable 47).

i. Support project planning of new projects with the customer base.

j. Stay abreast of industry trends and all applicable technologies, including scripting, security issues, authoring tools, graphic design tools, and new languages.

k. Analyze website traffic and recommend programming changes and manage transfer of files and memory allocation for website on the server; this data shall be reported in an automated reporting mechanism through a dashboard capability (Section F, Deliverable 44).

C.5.4.3.1 SUBTASK 3.1 – SUPPORT MAINTENANCE OPERATIONS

In support of maintenance operations, the contractor shall test and apply IAVM patches and remediation before the date given in the IAVM alert. The contractor shall also comply with IAVM reporting procedures. The contractor shall maintain a mounted file system installation shared across all respective environments (production, contractor test, stress test, quality assurance, development test, etc.). The contractor shall also perform log analysis, error detection, and fault correction on all web servers.

C.5.4.3.2 SUBTASK 3.2 – SUPPORT IA-COMPLIANT NEW SERVER BUILDS

In support of IA-compliant new server builds, the contractor shall perform the following tasks:

a. Configure and confirm functionality of web servers within 72 hours of request. Web servers will be IA compliant, built according to STIGS, patched, and approved for production use by the Cybersecurity Pre-Production Scanning Process.

b. Create and remove systems-hosted Uniform Resource Locator (URL) addresses. For new secure and non-secure URLs created on web servers, they shall be configured and functioning within 14 workdays of the request date and conform to DISA standards for URL security.

c. Complete a migration of production web applications within the systems enclave to bi-locational single URL address (one application per URL) and support the ongoing transition of the remainder within the established project timeline.

C.5.4.3.3 SUBTASK 3.3 – SUPPORT APPLICATION SERVERS

The contractor shall test and apply mandated IAVM patches and remediation before the date given in the IAVM alert. The contractor shall comply with IAVM reporting procedures. The contractor shall perform log analysis, error detection, and fault correction on all application servers. Web application technology configuration shall be 100 percent consistent with current production application servers. The contractor shall build application servers according to STIGs, patched, and approved for production use by the Cybersecurity Pre-Production Scanning Process.

C.5.4.3.4 SUBTASK 3.4 – PROVIDE DEPLOYMENT SUPPORT

The contractor shall provide IT deployment support. The contractor shall assess all failed or non-functioning deployments and prepare for redeployments to all environments.

The contractor shall perform all activities for “first time setup” on newly deployed applications within the web application technology environments. This shall include:

a. Domain initialization and configuration.

b. Managed Server initialization, configuration, and clustering.

c. Listener context root configuration.

C.5.4.4 SUBTASK 4 – PROVIDE DATABASE ADMINISTRATION SUPPORT

Database administration is the function of managing and maintaining Database Management Systems (DBMS) software. DBMS software such as Oracle, Sybase, Mongo and Microsoft Structured Query Language (SQL) Server need ongoing management or high-level administration. DMDC Systems database administrators (DBA’s) focus on the following aspects of database administration: DBMS installation, configuration, capacity planning, monitoring, patching, upgrades, backups, restores, refreshes, performance optimization, maintenance, set up, and response to alerts from monitoring tools, and DR.

The contractor shall provide database administration support for the current enterprise DMDC operating environments to include Oracle (version 11g or higher), Microsoft SQL (version 2008 R2 or higher), Sybase Adaptive Server Enterprise (version 15.0 or higher), NoSQL, Mongo, Hadoop, and MySQL platforms. The contractor shall develop technical specifications, design, develop, modify, test, and manage databases in DMDC’s multi-tier application architecture. The contractor shall monitor and optimize database performance and tune database operations. The contractor shall also ensure that data integrity facilities for databases are executed and that application developers are aware of any anomalies upon discovery.

The contractor shall ensure that applications, interfaces, extensions, forms, and reports integrate with database architectures. The contractor shall perform administration of database, storage management, high availability, and replication like ASM, RAC, DataGuard, GoldenGate, SymetricDS and GRID technologies.

The contractor shall provide Database Administrators and UNIX system administrators that shall be required to work together to manage the Exadata high availability replication, storage cells, and database compute nodes as a whole integrated system. Exadata requires close management and coordination among various ITOPS groups and the Oracle Exadata team. In order to perform database administration, the contractor shall have an understanding and be able to work with various OS environments and understand DR requirements and processes. The contractor shall also understand capacity planning as it pertains to databases and be able to administer Oracle EXADATA database systems. The contractor shall assess, design, deploy, and operationalize DMDC’s mission-critical workloads that are currently being supported by all databases.

Additionally, in support of database administration, the contractor shall perform the following tasks:

a. Perform reverse engineering when database corruptions occur or as a result of troubleshooting systems and restore databases to uncorrupted versions.
b. Provide detailed technical direction to application developers and stakeholders who have been assigned to assist with modifications or changes to the computer programs involved.
c. Deliver implementation plans that provide the detailed approach taken when implementing new database features, versions, and/or capabilities. Define and administer quality control methods and draft detailed and comprehensive documentation covering user requirements, system design, new software, and software modifications.
d. Create and test backups of data, provide data cleansing services, verify data integrity, and implement access controls.
e. Develop implementation plans for continual availability improvements of database services. Every effort shall be taken to minimize unavailability of the database services.
f. Develop, manage, and support the SQL databases used for the DMDC web, SharePoint sites, portals, and supporting SQL databases. The contractor shall provide technical guidance and advice to division webmasters.
g. Provide application deployment support, analysis for performance improvements in procedure or application processing flow, automated scheduling, and statistical trends.
h. Create and maintain run books that define SOPs for all provided services for setup and configuration of applications, deployments of applications, application startup order of dependencies, and health-monitoring requirements to ensure availability.
i. Engage with database vendors to validate and deliver a plan of action that will take DMDC from its current state to the proposed future architecture in alignment with DMDC’s application migration and strategic plan (i.e., fit into DMDC’s future direction).
j. Implement log management security correlation engine to protect DMDC from external threats such as bots and worms and internal risks such as fraud and theft.

The contractor shall perform monitoring and optimize the performance of all DMDC databases; this shall include the following activities:

a. Planning for backup and recovery of database information.
b. Maintaining archived data on tape.

c. Backing up and restoring the database.
d. Contacting all database vendors for technical support as required.
e. Conducting high availability administration RAC backup, recovery, performance tuning, and troubleshooting of production, DR, and test RAC databases.
f. Creating and supporting databases across internal and end-user applications, improving database integrity through quality assurance, and managing change control processes related to the Oracle environment.
g. Analyzing, testing, coordinating, and facilitating patching needed to maintain cyber security compliance.
h. Analyzing existing database applications for improvements, database tuning, and monitoring The contractor shall work with application developers to integrate efforts with relational databases, participate in team or company projects as required, maintain state-of-the-art knowledge of existing best practices in database administration, mentor/train lower-level database administrators, perform all tasks associated with DR exercises, perform capacity planning.
i. The contractor shall provide 24x7x365 on-call NOC support.
j. Developing and troubleshooting shell scripts as needed.
k. Ensuring recovery manager (RMAN) and backup processes and procedures are followed and maintained.
l. Providing monthly database storage utilization and capacity planning reports until such time as this information is available via the dashboard.

C.5.4.5 SUBTASK 5 – PERFORM NETWORK AND TELECOMMUNICATIONS MANAGEMENT

The network/telecommunication administrators are responsible for the day-to-day operations and maintenance of the DMDC Enterprise Network and Telecommunication Infrastructure. The administrators carry out responsibilities in some or all of the following technical areas: hardware and software maintenance, system upgrades, infrastructure design and layout, DR design and implementation, monitors, software patching, DoD and DMDC security policies maintenance, troubleshooting, training and or supervising staff; and offering technical support for projects.

The contractor shall monitor, administer, securely install, configure, and maintain network equipment such as routers, switches, firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), network encryption devices Tactical Fastlane (TACLANE) and Electronic Key Management System (EKMS)), load balancers, domain name system (DNS) appliances, and wireless infrastructure. This support shall be performed on the DMDC NIPRNET and SIPRNET in accordance with DoD, DMDC regulatory guidance and compliance standards and, when applicable, with the International Standards Organization (ISO).

The contractor shall identify, isolate, troubleshoot, correct, and document any/all problems within the DMDC Network and Telecommunication Infrastructure to include the Wide Area Network (WAN), Local Area Network (LAN), enterprise firewalls/routers/switches, load balancers, domain name system security extension (DNSSEC), private branch exchange (PBX)/VOIP and Remote Access Service (RAS) 802.1x,. The contractor shall provide Network Access Control (NAC)/Network Access Protection (NAP), manage, operate, and support the

Virtual Private Network (VPN) access for agency-to-agency connections and gateways to include remote access user requirements.

The contractor shall provide, secure, and maintain optimally configured telecommunication resources to support the DMDC enterprise at all sites. Support includes integration, installation, upgrades, decommissioning, patching, and service availability. The contractor shall perform escort services for carriers and perform test and turn up of new circuits. The contractor shall perform joint testing and troubleshooting with DISA, DoD network providers, and public carriers.

The contractor shall monitor all network and telecommunication infrastructure equipment to include circuits, nodes (physical and virtual), and hardware supporting the DMDC enterprise. The contractor shall securely rack, label and diagram, cable, configure, and maintain network and telecommunication infrastructure resources such as routers, switches (e.g., Juniper, CISCO, and Brocade Data Storage), firewalls, IA security devices, web proxies, F5 load balancers, global traffic managers, network and circuit encryption devices, and PBX/VOIP resources. Upon full VOIP implementation, the PBX will be decommissioned. This is applicable to current network and telecommunication infrastructure assets and future environments including emerging technologies.

The contractor shall monitor the status of all network devices and communication circuits and ensure all firewall rules incorporated strictly adhere to DoD Ports and Protocols Service Management (PPSM) guidelines for both NIPRNET and Secure Internet Protocol Router Network (SIPRNET) environments.

The contractor shall provide complete lifecycle support for DMDC enterprise network assets and configurations. The contractor shall ensure all approved network components are integrated and operate in accordance with Original Equipment Manufacturer (OEM) performance standards. Every effort must be taken to ensure the maximum amount of operational availability of network services. The contractor shall perform all network device administrative functions. All administrative operations shall be performed in a manner in which adverse impact on network availability is minimized and in accordance with established SOPs. Additionally, the contractor shall perform all security configurations and operations in accordance with the DoD Instruction (DoDI) 8500.01 and compliant with any additional DoD Instructions, U.S. Cyber Command (USCYBERCOM) Orders, Federal Information Security Management Act (FISMA), and DMDC policies.

Additionally, in support of network and telecommunications management, the contractor shall:

a. Review and validate all telecommunications circuits and formulate recommendations for retention, cancellation, or transfer of responsibility.
b. Maintain a real-time database of the installed equipment detailing equipment descriptions, serial numbers, quantities, locations, maintenance levels, circuit IDs and inventories, and POCs, as well as tracking all network router installations to include equipment descriptions, serial numbers, quantities, locations, maintenance level, circuit inventories, and firmware versions.
c. Optimize performance, perform system station back-ups on a weekly basis, and recover, configure, and connect hardware.

d. Develop, propose, and implement plans for continual availability improvements for the network and telephony services and administer availability of telephony infrastructure. The contractor shall support telephony requests and incidents.

e. Respond to receipt of a notification of outages, disruptions, or failures within 10 minutes.

f. Maintain an accurate cabling to network switch port inventory ensuring any and all changes deployed in data centers (primary and secondary), and remote sites are updated within five workdays. This is to provide an up-to-date inventory or documented mapping of all cable runs to network switches to aid and assist in any troubleshooting efforts.

g. Monitor and report on the overall health of the system infrastructure, to include equipment attached to the network and all applications directly supporting the network. Support shall include interacting with DISA to provide technical assistance via phone or email.

Note that any scheduled VOIP outages will be approved by the Government and adhere to ITOPS SOPs to ensure visibility and proper coordination.

The contractor shall troubleshoot and resolve all LAN/WAN issues. Devices to be administered include:

a. Firewalls

b. Switches

c. Routers

d. VPN appliances

e. Load balancers

f. Secure Socket Layer (SSL) accelerators

g. Online Certificate Status Protocol (OCSP) servers

h. Host/network intrusion detection devices

i. IA security devices

j. Network management software that is part of the interface between the administrator and the network appliances

k. Analog, digital, and IP Phones

l. 802.1x/Certificate Authorities – to meet DoD regulations, DMDC must employ Institute of Electrical and Electronics Engineers (IEEE) 802.1X NAC across the DMDC Enterprise (NIPRNET and SIPRNET).

m. Network Access Protection (NAP) – Standup and maintain a Government-approved NAP infrastructure using DMDC-provided IA software.

n. Network Access Control (NAC) - Standup and maintain a Government-approved NAC solution to authenticate DMDC workstations using certificates derived from a DMDC-controlled Certificate Authority.

The contractor shall develop and present for approval implementation plans for continual availability improvements of network services and track change management activities that impact network administration functions annually, with the first report being 90 days after TO award (Section F, Deliverable 47). The contractor shall conduct device firmware patches, OS patches, device configuration file changes, device installation, decommission, and support for issues related to network devices and servers to support VoIP within the DMDC enterprise enclave.

The contractor shall implement and maintain security configurations for all DMDC enterprise network assets and configurations. All security configurations and operations shall be in accordance with DoDI 8500.2 and compliant with any additional DoD Instructions, USCYBERCOM Orders, FISMA, and DMDC policies. The Cybersecurity Division will detect any deviations as part of regular scanning and auditing. The contractor shall respond to any issues with either a fix or adequate justification for non-compliance which is accepted and approved by the DMDC cybersecurity staff. Additionally, the contractor shall be proactive and coordinate any non-compliance issues in advance of identification by the cybersecurity division. Any decision to not apply any STIG configuration setting shall be approved by the cybersecurity division.

Additionally, the contractor shall:

a. Perform network cabling. This shall include management of the cabling between network devices and servers, cablings from the network operations centers to the wall plates, and connectivity from the wall plates to the end-user workstation.
b. Support secure and non-secure voice networks consisting of user telephone instruments, Secure Telephone Equipment (STE) instruments, and Cisco 7945 phones serviced by Enterprise Classified Voice over IP (ECVoIP), unclassified VoIP network and instruments. The contractor shall provide onsite troubleshooting, problem isolation, and service restoration.
c. Coordinate maintenance and repairs with vendors per published schedules or when necessary, due to hardware or software failures.
d. Provide and monitor remote teleworker access and performance. The contractor shall recommend changes and technology upgrades which will improve performance for remote-access customers.
e. Support the physical racking, power-on, and cabling of new or relocated servers to successfully integrate the hardware into the operational environment.
f. Support the asset management process with removing servers from racks, removing and degaussing hard drives, and palletizing equipment in preparation for DRMO during decommissioning.
g. Address and remediate vulnerabilities identified in Assured Compliance Assessment Solution (ACAS), the DMDC/DoD vulnerability management tool managed by the Cybersecurity Division.

The contractor shall provide a certified COMSEC manager and alternate. The contractor shall acquire, integrate, and test COMSEC equipment and handle COMSEC keys in accordance with the National Security Agency (NSA), COMSEC, and key management directives. Support is required to include accountability, issue, operation, destruction, turn in of all COMSEC key material and equipment, and re-key operations.

The contractor shall:

a. Perform as a COMSEC POC and track all actions involving COMSEC management and support the maintenance of COMSEC accounting records.

b. As requested, prepare reports concerning COMSEC incidents in accordance with Government regulations and COMSEC maintenance forms, logs, and reports pertaining to COMSEC material accountability.

c. Maintain up-to-date knowledge of the Key Management Systems (KMS) and specialized hardware and software programs used to generate and maintain COMSEC material.

d. Handle daily operational matters based on the knowledge of COMSEC management and use that knowledge to refer inquiries to appropriate personnel.

e. Provide support on COMSEC matters pertaining to the use of secure communications devices.

f. Maintain cryptologic equipment in operational condition and coordinate with DMDC IT engineers to address outages resulting from equipment failure, failed re-key transactions, and other issues that can affect network and system availability.

C.5.4.6 SUBTASK 6 – CONDUCT MAINFRAME SUPPORT SERVICES

DMDC operates an IBM z10 series mainframe currently located at the Naval Postgraduate School (NPS) in Monterey, CA. The system provides computational analysis and supports DMDC and other tenant organizations with computing and networking services. The mainframe operates up to two Logical Partitions (LPARs). The mainframe consists of one IBM Production System-ZOS production partition one z/OS development partition. DMDC's current mainframe hardware reaches end of life September 30, 2020. As a result, this subtask will not be required after October 1, 2020. DMDC is currently considering alternate courses of action to address this issue.

The contractor shall provide personnel with extensive knowledge and experience with the installed IBM mainframe system and application software. The majority of work can be performed remotely; some hands-on work shall be required onsite. Additionally, personnel shall have expert understanding of IBM's zSeries mainframe, LPAR configuration, and alternative workload structure.

The contractor shall manage the technical lifecycle of the z/OS software product, package, or subsystem assigned. This involves the full spectrum of the technical lifecycle of these entities, including requirements determination, technical design, prototyping, performance prediction/modeling, installation, customization, problem management, documentation, security compliance, change control, regression avoidance, license-key management, single-point-of-failure elimination, recovery automation, and assured availability.

The contractor shall assist DMDC in the configuration of Resource Access Control Facility (RACF) Support. The contractor shall provide IBM z/OS System programming, maintenance, and configuration support. Third-party systems software installed shall be kept compliant with current OSs. New software may be required as a result of customer requests, standardization, or vendor directives. The contractor shall monitor functioning of the current mainframe, ensuring that current mainframe is running up to standards established by the OEM.

Additionally, the contactor shall perform the following activities:

a. Support the working of installed software and firmware including system software, utilities, programming languages, compilers, interactive terminal software, and transaction processing software. The contractor shall provide technical and engineering support in z/OS.

b. Perform trend analysis quarterly on system performance, recommend configuration, and assist in the coordination and planning to schedule system upgrades (Section F, Deliverable 50). Coordination may include DMDC and other agencies at DMDC's direction.

c. Conduct analysis, installation, and testing of all new software releases.

d. Provide technical and user training to DMDC technical staff and end-users.

e. Provide technical support for the problem resolution process to resolve errors in system software and coordinate and transition from one hardware subsystem to another as scheduled.

f. Perform product installs. The contractor shall research problems and keep current on available patches, fixes, releases, and lifecycle (going-out-of-support) plans. The contractor shall track problems turned over to vendors for resolution and escalate attention to the problems where appropriate.

g. Coordinate with DMDC staff to ensure overall efficiency and effectiveness of the mainframe operation.

h. Provide on-call support including answering questions, troubleshooting, and availability to repair problems 24x7x365 in coordination with the virtual NOC.

i. Perform weekly system backups every Sunday to ensure adequate protection of data in accordance with applicable DoD and DMDC directives. The contractor shall ensure backup data is archived for a period conforming to DMDC dataset storage naming conventions. The contractor shall also document in a log the activities and actions taken. The contractor shall accomplish backups daily, weekly, monthly, semiannually, and annually. The log shall be available to the Government on request. Data restores shall be verified every 180 calendar days. All information assurance appliances and systems shall be backed up to ensure proper and expedient service restoration in the event of a system outage (Section F, Deliverable 48).

j. Perform system control and tape library functions to include locating and storing media, reorganizing files as necessary, informing DMDC of input data errors, and scheduling due-in or due-out machine workloads.

k. Provide IBM z/OS programming, maintenance, and configuration support. The contractor shall complete 98 percent of software updates within 30 calendar days after receipt of software.

l. Conduct ongoing problem reporting/monitoring, status updates, software/hardware incident logs, capacity planning processes and procedures, etc. The contractor shall update the information on the DMDC ITO SharePoint site weekly.

m. Coordinate with DMDC and other agencies at DMDC's direction to ensure overall efficiency and effectiveness of the mainframe operation.

n. Maintain and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. The contractor shall resolve abnormally ended jobs caused by conditions external to production programs.

o. Enhance processing capabilities and efficiencies through system tuning and other run-time improvements. The contractor shall analyze performance metrics and respond proactively to potential problem areas.

p. Attend monthly meetings of Mainframe Users Group and work with DMDC and other agencies at DMDC's direction on issues raised in the meeting.

q. Recycle computer tapes, initialize new ones when needed, and retire tapes that are beyond their useful life.

r. Work with hardware repair personnel to ensure that problems with equipment are resolved.

s. Perform the following duties for job scheduling technology: install and maintain software, set up RACF security, troubleshoot user and system problems, train personnel in use of job scheduling technology, and automate production jobs and system maintenance.

t. Perform the following duties for secure data transfer software: install and maintain software, set up security for transfers, configure/change nodes for transfers, troubleshoot problems, and set up new transfers and test new connections.

u. Assist in the communication with external agencies and customers to establish the best secure solution for electronic data transfers based on their hardware architecture and software capabilities.

v. Maintain, assist, and coordinate with end users using the mainframe's automated schedule tool.

w. Assist in the creation of login IDs, permissions, and updated internal documentation for public IP addresses; gather POC names, email addresses, and phone numbers of agencies connecting with the mainframe.

x. Work with DMDC and other agencies at DMDC's direction to establish connectivity with outside agencies through the network to connect to the mainframe. The contractor shall ensure that DMDC and other agencies at DMDC's direction receives IP address and POC information and that connectivity testing for both test and production environments between DMDC and outside agencies is conducted.

y. Performance/Routing Enterprise Extender Network to support data transmission using Cyberfusion to the SSA network. The contractor shall update and maintain Virtual Telecommunications Access Method (VTAM) z/OS environments.

z. Install, configure, implement, and manage Transition Control Protocol/Internet Protocol (TCP/IP) and its associated servers in the z/OS environment. The contractor shall coordinate TCP/IP HW/SW configurations in the z/OS environment, IP addresses, and VPN requests with the NOC to include in their firewall configuration. The contractor shall also monitor network components and resolve hardware, software, and interoperability issues.

aa. Delete inactive accounts and manage active accounts.

bb. Work with Time Sharing Option (TSO) OS with the z/OS environment. The contractor shall edit, modify, and create jobs executing within this environment.

cc. Work with Unix subsystems within the z/OS environment.

dd. Assist in the creation, changes, and troubleshooting problems with Job Control Language (JCL) and batch processing jobs within the z/OS environment.

ee. Manage, monitor, and diagnose system problems for the z/series IBM server for computer operations.

ff. Participate in the planning and procurement of new systems for hardware and software. The contractor shall review procedures and technical specifications to determine if requirements needs have been achieved.

gg. Assist in identifying critical IT systems, services, and business applications; developing a recovery strategy; reviewing onsite and offsite backup policies, procedures and standards; developing, documenting, and maintaining a recovery plan; preparing SOPs; and presenting information to management.

hh. Meet with the Mainframe Accreditation Team to discuss and plan installation of DISA's requirement to implement procedures in the appropriate STIG for z/OS. The contractor shall review Access Control (AC), Audit and Accountability (AU), Security Assessment (CA), configuration management controls, and all other controls.

ii. Install, configure, customize, implement, and manage the Data Facility Storage Management Sub-systems (DFSMS) for Removable Media Services (RMS) for access to IBM's 3494 Automatic Tape Library (ATL) Data Server. The contractor shall integrate server virtual machines and tape management software applications to interface with RMS for backup and recovery of data. The contractor shall interface and monitor the ATL environment via its Library Manager console.

jj. Customize input/output (I/O) hardware definitions for LPARS, Open Systems Adapter (OSA), and Channel Path Identifier (CHIPIDS) to specify channel paths installed on the Central Processor Complex (CPC), the control units attached to these paths, and the I/O devices assigned to the control units and Fiber Connection (FICON) and Enterprise System Connection (ESCON) definitions to access the manual tape drives, ATL drives, and Direct Access Storage Devices (DASD).

kk. Implement the proper security patching and STIG implementation to be able to maintain an ATO from DMDC's Authorizing Official.

ll. Create, review, and maintain SOP documentation.

C.5.4.7 SUBTASK 7 – SECURITY COMPLIANCE AND PATCH MANAGEMENT SUPPORT

Security compliance and patch management is a crucial element in systems administration and ITOPS. IT security planning, implementation, and compliance is integral to all work performed at DMDC and, therefore, coordination with DMDC stakeholders and the Cybersecurity Division within DMDC is critical to ensure that patches to vulnerabilities are quickly remediated. GOTS application security compliance and patch management is not within the scope of this TO.

C.5.4.7.1 SUBTASK 7.1 – SECURITY COMPLIANCE

The contractor shall perform IAVM compliance patching on all servers, workstations, and all other IAVM applicable assets on both the SIPRNET and NIPRNET networks. Remediation is to be completed according to Joint Force Headquarters DoD Information Networks (JFHQ-DoDIN)

IAVM guidelines. The contractor shall report IAVM patch compliance and submit to IAVM POA&Ms to the Cybersecurity Division according to reporting guidelines.

The contractor shall ensure all vulnerabilities identified by DMDC vulnerability scanning tools, which is currently the ACAS, and Security Compliance Checker/Security Content Automation Program (SCC/SCAP) scans, which are conducted by the Enterprise Services, Cyber Division, are remediated or mitigated, or the contractor shall submit a STIG deviation/non-compliance form and POA&M.

The contractor shall implement, maintain, and comply with USCYBERCOM and JFHQ-DoDIN Orders and Directives. Implementation shall be completed according to USCYBERCOM guidelines and submitted by the Cybersecurity Division. The contractor shall provide active participation of SMEs to cybersecurity working groups sponsored by the Cybersecurity Division in response to JFHQ- DoDIN Orders and Directives.

The contractor shall provide support for internal and external audits, pen testing, red team testing, and other security reviews. This shall include subject matter expertise, documentation, supporting requests for accounts and access that have been approved by DMDC's Authorizing Official, and participation in interim project reviews (IPRs).

The contractor shall ensure that all DMDC IT assets meet STIGs compliance prior to operating on the DMDC network. The contractor shall implement, apply, and maintain STIG configuration to all IT assets. Deviations from STIG configuration setting shall follow the DMDC STIG deviation process and be approved by the Cybersecurity Division.

The contractor shall ensure that all new IT assets built under this TO and baseline images go through the DMDC pre-production process and are approved by the Cybersecurity Division prior to operation in a production environment.

Additionally, the contractor shall:

a. Install, configure, and test patches and changes required by IAVM issuances, vendor patches, and STIG configuration items. The contractor shall implement all necessary changes to enterprise software and equipment in accordance with the suspense date articulated by the Cybersecurity Division.
b. Remediate software vulnerabilities (not including GOTS applications) and system misconfigurations identified in the DMDC vulnerability management tool managed by Cybersecurity Division.
c. Submit STIG deviation/non-compliance and provide a POA&M for remediation actions that cannot be accomplished by the Cybersecurity Division assigned completion date.
d. Provide a STIG Deviation/Non-Compliance Report for system configuration items that cannot be accomplished by the Cybersecurity Division assigned completion date.
e. Develop and implement a patch management plan, excluding GOTS applications, that will test and remediate vulnerabilities within the DoD timeline (in accordance with NIST SP 800-37 and as directed by USCYBERCOM (USCC) Task Order (TASKORD) 13-067). Vulnerabilities shall be remediated for critical findings within seven calendar days of discovery, high-level findings within 21 calendar days of discovery, medium-level findings within 60 calendar days, and low-level findings within 90 calendar days of discovery or in accordance with DMDC-mandated timelines.

f. Ensure that STIG configuration items are to be corrected upon identification by the Cybersecurity Division.
g. Gather and collect data to support reporting of IAVM and Federal FISMA USCC/JFHQ orders and directives, DoD CIO directives.
h. Ensure that any exceptions and security non-compliance activity are processed through and approved by the Cybersecurity Division.
i. The contractor shall perform Vulnerabilities Disclosure Program (VDP) patching, remediation, and reporting to comply with DMDC Cybersecurity Vulnerability Disclosure processes and guidelines.

C.5.4.7.2 SUBTASK 7.2 – PATCH MANAGEMENT

The contractor shall perform patching on all assets. The current primary software tools that support patch management are Tanium, Puppet, and System Center Configuration Management (SCCM). The contractor shall apply vendor-supported patches (security and software) on a continuous and timely basis per DoD and DMDC policy. The contract shall support updates to third-party software listed in the DTL to all applicable DMDC IT assets (e.g., network, servers, and workstations).

The contractor shall ensure that all workstation and server patches are completely deployed to all assets, to include laptops, desktop workstations, servers, tablets, etc. Patches shall be thoroughly tested for a period of one week on Government-approved test machines. Patches shall be deployed NLT 14 days after the patch is released, or by the stated deadline presented by DISA/IAVA release management. The contractor shall report to DMDC-designated Government personnel a status of its efforts as requested by management.

Additionally, the contractor shall:

a. Ensure all DMDC IT assets have the required cybersecurity monitoring tools (e.g., tripwire agent, Host Based Security System (HBSS) agent) installed and operational in accordance with DoD and DMDC policy. The contractor shall assist and troubleshoot with cybersecurity tools (e.g., HBSS security staff, ACAS, and others).
b. Ensure that all software or hardware patches, updates, and firmware must come from the DoD patch repository as applicable. Exceptions shall be approved by the Cybersecurity Division prior to engagement.
c. Provide applications services that are in compliance with and support DoD Public Key Infrastructure (PKI).
d. Provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Solutions shall comply with NIST, Federal Information Processing Standards (FIPS) standards, and DoD or IC standards.
e. Coordinate patches or changes that require system or application downtime with the Government and schedule during allotted maintenance hours.
f. Participate in annual audits of accounts and privileged user activity and provide recommendations on access and controls.

C.5.4.7.3 SUBTASK 7.3 – RISK MANAGEMENT FRAMEWORK (RMF) SUPPORT

The contractor shall support DMDC risk management activities including Security Test and Evaluations (ST&E), system documentation, authorizations, risk assessments, compliance with NIST 800-53, and threat assessments in accordance with DoD RMF and processes. The contractor shall manage documentation for all DMDC IT assets (e.g., infrastructure, networks, interconnections, commercial software, custom-developed applications, systems, and frameworks) as required by RMF.

The contractor shall ensure that Enterprise Mission Assurance Support System (eMASS) artifacts are developed and maintained concurrently throughout the system lifecycle, beginning at inception of new IT activities. These will include system-level controls and common controls that will be inherited by individual applications.

The contractor shall prepare and maintain the artifacts required to support the RMF packages that achieve an ATO determination, including physical security plans of IT sites and facilities, system descriptions, diagrams, data flows, POA&M, security assessment reports, Authority to Connect (ATC) circuit accreditation, and other documentation. RMF artifacts shall be updated as required and reviewed annually for accuracy and completeness with updates being made as required.

The contractor shall support security incident response team requirements and make recommendations to the DMDC Cyber Incident Response Team (CIRT) on additional actions or corrections to improve the security posture of DMDC.

C.5.4.7.4 SUBTASK 7.4 – PORTS PROTOCOLS AND SERVICES MANAGEMENT (PPSM)

The contractor shall support PPSM to include the following:

a. Manage, review, and submit PPSM registry requests; register data communication modes identifying the Ports, Protocols, Application Services (PPS) used and the network boundaries crossed. The contractor shall support PPSM auditing and ensure existing and new registration requests do not violate Connection Approval List (CAL) and DoD requirements.
b. Review and submit PPSM registry requests, collect data, review firewall requests for compliance with DoD requirements. The contractor shall identify errors, deny non-compliant requests, and approve and deny request based on CAL.
c. Support the Connection Approval Process (CAP), Systems/Network Approval Process (SNAP)/Global Information Grid (GIG) Interconnection Approval Process (GIAP), collect data, and process CAP and SNAP/GIAP requests.
d. Ensure all requests meet current DISA guidelines. Data collection information is determined by DISA and subject to change without notice to DMDC. Current guidelines include RMF artifacts, topology diagram, locations, and circuit connections.
e. Provide expertise to manage CAP and SNAP/GIAP; obtain and submit accounts and provide feedback on approvals and denials. The contractor shall respond to deficiencies and monitor renewals.
f. Support DISA White List Management, manage DISA Whitelisting, and collect data to process and register asset and application whitelisting. The contractor shall provide feedback on IA approvals and denials and submit whitelist request to DISA.

C.5.5 TASK 5 – CUSTOMER SERVICES SUPPORT

Customer services provides support to DMDC end users of the IT infrastructure which includes desktops, laptops, and software; printers; document scanners; audio-visual equipment/VTC; and handheld devices. The contractor shall operate a customer helpdesk to serve as the single POC to answer IT/IM trouble calls. This also includes support for registration authority PKI tokens, peripheral administration, and support to end-user devices.

C.5.5.1 SUBTASK 1 – PROVIDE HELPDESK SERVICES

The DMDC ITOPS enterprise helpdesk is responsible for providing basic application software and/or hardware support to internal DMDC callers. This helpdesk represents the customer-facing component of the ITOPS Division by serving as a portal and conduit for all internal DMDC customer inquiries. The helpdesk responds to inquiries pertaining to the DMDC IT infrastructure such as hardware, software, user account security, communications, and ITOPS policy guidance to end users. Some of the support and services provided include support to DMDC end users of the IT infrastructure which includes desktops, laptops, and software; printers; document scanners; audio-visual equipment/VTC; and handheld devices. The contractor shall operate a Tier I, consolidated customer helpdesk to serve as the single POC to answer IT/IM trouble calls for approximately 3,000 DMDC end users.

The contractor shall operate a Tier I helpdesk serving as the frontline in supporting DMDC’s IT. The helpdesk staff shall be trained in preliminary diagnostics and resolution of common issues on end-user devices. The key high-level objectives are to improve customer service, resolve Tier I issues, expeditiously, and provide end-user self-service abilities.

The contractor shall assess the existing self-help capability and improve or re-develop and maintain an automated, on-line, easily accessible, user self-help feature, including a Frequently Asked Questions (FAQ) list, with the intent of reducing the need for users to contact the service help desk. The contractor shall draft, for Government approval, IT topics of interest, notices, and technical help to users across the DMDC enterprise. The contractor shall adopt knowledge databases and best practices in the areas of customer reporting, logging, tracking, and resolving of IT problems and service requests.

Additionally, in support of helpdesk services, the contractor shall perform the following:

a. Staff the helpdesk operations from 0600 to 2100 hours Eastern Time (ET), Monday through Friday. Staffing shall be provided to places of performance as listed in Section F.2. Staffing shall be based on expected need and adjusted to maintain acceptable performance.

b. Routinely update and manage all helpdesk tickets, ensuring tickets are documented concisely and closed within timeframes for routine, regular, urgent, critical, and emergency in accordance with the PRS.

c. Maintain and update checklists and/or scripts in high-focus incident/request areas ensuring continuity with all helpdesk personnel at the Mark Center and DoD Center Seaside.

d. Monitor, manage, and optimize user call queues and responses to service helpdesk phone calls.

e. Upon receipt of a customer's trouble-call, open a ticket, perform the required assessment, and either answer the question, use remote access to troubleshoot, isolate, and resolve the problem or refer to the next tier level of help.

f. Document all tickets using the current incident, request, problem, and change order categories to capture category/volume.

g. To the extent feasible, resolve customer problems and respond to customer requests while on the telephone with the customer.

h. Only close trouble tickets after the issue/problem has been resolved. Service helpdesk tickets not operated by the contractor shall be relayed to the appropriate personnel and are not subject to SLA measures for ticket closure or incident and problem resolution.

i. Confirm with each customer that his or her problem has been resolved and verify customer satisfaction with service provided, though email or other automated means.

j. Perform predictive analysis to anticipate changes in call volume (i.e., major evolution of software).

k. Respond promptly to user calls for assistance, giving first priority to staff work stoppages.

l. Add, set up, and delete user accounts; unlock accounts when appropriate.

m. Provide daily ticket queues and Very Important Person (VIP) support status to Government customer service leads via dashboard, email updates, and in person where required. There are approximately 30 VIP identified employees. The majority of these individuals are located at either Mark Center or Seaside locations.

n. Develop a weekly status report of all helpdesk tickets and the progress of resolution efforts (Section F, Deliverable 51).

o. Notify the Government of all work requests that take longer than 24 hours to resolve in a daily (Monday through Friday) exception report. If requests require hardware or software that is not currently available, notify the Government as soon as the shortfall is identified. The contractor shall notify the Government of tickets classified as urgent or above.

p. Upon request by the Government, obtain a customer satisfaction report and closeout confirmation for each incident, periodically survey users for overall satisfaction, and support third-party or independent user surveys and quality assessments.

The contractor shall provide DoD Enterprise Email (DEE) Support. The DoD Enterprise Email (DEE) service is provided by DISA and serves as a secure cloud-based email to DMDC. DISA's DEE service desk provides Level II, Tier II support to an organization's Level I, Tier II and III end-user support. DISA integrates DMDC into the operational structure and provides 24x7x365 support through their central service helpdesk, reference virtual NOC requirement.

The contractor shall provide Tier I and II support for email services provided by DISA. Tier I support will be through the DMDC helpdesk and will collect information regarding DEE. Tier I support shall also be the primary team creating and maintaining user accounts, Non-Personnel Entities (NPE), and distribution lists for DMDC using DISA's Defense Enterprise Provisioning Online (DEPO) service, Outlook Web Access (OWA), and possible other tools as they become available.

C.5.5.2 SUBTASK 2 – DMDC REGISTRATION AUTHORITY (RA) SUPPORT

The DMDC RA provides PKI activities for the DMDC Enterprise for the NIPRNET and SIPRNET environments. Services provided are SSL certificates, domain controller certificates, alternate tokens, group certificates, code signing certificates, SIPRNET tokens, key recovery, and External Certificate Authority (ECA) certificate processing. Personal Identification Number (PIN) reset services are provided for tokens that are issued by the DMDC RA.

The contractor shall provide RA services in compliance with, but not limited to, DoD Certificate Policy, DoD PKI Certification Practice Statement, DoD National Security Service (NSS) Public Key Infrastructure (PKI) DoD Registration Practice Statement, and DoD Directives. The contractor shall designate RA officers who shall be responsible for duties of certificate issuance, certificate revocation, or key recovery in both the NIPRNET and SIPRNET environments at DMDC Seaside and the Mark Center. The contractor's personnel designated as the DMDC RA shall obtain their DoD PKI RA credential, and/or NSS DoD PKI RA Credential, and/or JITC RA credential. The contractor personnel designated as the DMDC RA shall have a Secret clearance and be knowledgeable of certificate policies and IA concepts, practices, and procedures.

The contractor shall designate local RA, Trusted Agents, System Administrators and additional RA Program stakeholders at various DMDC-supported sites to support RA services. The contractor shall partner with other ITO groups, DMDC divisions, local security office or agencies to provide RA Program services. The contractor shall perform RA Program duties on-site in a secured location, according to the Certification Practice Statement (CPS) and Registration Practice Statement (RPS), during core business hours as coordination is necessary with certificate requestors.

The contractor shall provide RA services in the NIPRNET and SIPRNET environment including, but not limited to, SSL certificates, Domain Controller certificates, MultiSAN certificates, alternate tokens, code signing certificates, group certificates, SIPRNET tokens, key recovery, and ECA certificate processing. Certificate requests shall be processed based upon the established DMDC RA Program SOPs.

The contractor shall be responsible for processing certificate request through the DMDC change management process. This includes certificate signing request (CSR) file testing, documentation verification, troubleshooting with certificate stakeholders, guiding the request through the change management process, certificate submission to the certificate requestor, and documentation close-out.

The contractor shall be responsible for the development and maintenance of RA Program documentation including, but not limited to, policies, procedures, standards, checklists, forms, and NIPRNET/SIPRNET certificate tracking spreadsheets. This shall also include maintenance of the DMDC RA internal and user SharePoint webpage. The contractor shall maintain email groups and SharePoint access groups related to the DMDC RA Program to limit access to only required DMDC RA Program stakeholders. The contractor shall maintain the internal RA Program records to include, but not limited to, RA Training Certificates, Program Approval Letters, and DMDC RA PKI Program Role List.

The contractor shall provide token services in the NIPRNET and SIPRNET environments. For the NIPRNET, token services include, but are not limited to, alternate tokens and code signing tokens. For the SIPRNET, token services include, but are not limited to, SIPRNET tokens.

Token services also include, but are not limited to, enrollment and registration of token users, maintaining token inventory, PIN resets, and providing current disposition of token services. The contractor shall issue tokens via in-person issuance at a DMDC or approved site or secure, trackable account means (e.g., FedEx) at the cost of the Government.

Additionally, the contractor shall be responsible for the following:

a. Providing reports such as the Certificate Expiration Annual Report, RA Program Monthly Reporting, RA Program Annual Report, and other ad hoc reporting(Section F, Deliverables, 52, 53, 54, and 55).
b. Tracking the lifecycle of all certificates issued by the DMDC RA Program. Certificate Expiration tracking activities shall include, but are not limited to, annual report of certificate expirations, monthly email notifications to the DMDC Certificate Board, and certificate expiration escalation.
c. Development and execution of training sessions for RA Program and RA Program stakeholders and team members, as needed.
d. Attendance at various meetings, developmental projects/activities, and learning opportunities related to the RA community and duties at the direction of the Government.
e. Responding to data calls, as requested.
f. Researching and submitting to the Government requests through the DMDC standardized procurement process to procure supplies, equipment, and commercial certificates in support of the RA Program.
g. Executing program activities to include, but not limited to, preparing and participating in an RA Program Audit by DISA.
h. Maintaining audit readiness; audits may be performed by DMDC or external oversight authorities without advance notice.

The contractor shall safeguard all RA equipment, information, and property. At the close of each work period, Government facilities, equipment, and materials shall be secured. The contractor shall be responsible for any travel-related expenses for designated RA personnel to obtain their DoD PKI RA Credential, and/or NSS DoD PKI RA Credential, and/or JITC Registration Authority Credential.

C.5.5.3 SUBTASK 3 – SUPPORT END-USER DEVICES AND AUDIO/VISUAL ADMINISTRATION

C.5.5.3.1 SUBTASK 3.1 – SUPPORT END-USER DEVICES

The scope of this task is to provide end-user device services and support to DMDC users located at the Headquarters office in the NCR as well as other DMDC locations, remote users, and alternate work locations. Note that locations and users are fluid and may change over the life of the contract. DMDC infrastructure includes approximately 2,200 desktop Personal Computers (PCs), 500 laptops, and 250 handheld devices (e.g., BlackBerry and other smartphones, and tablets). At this time, approximately 910 PCs are located in Seaside, CA, 680 PCs in the NCR, 50 PCs in TX, 2 PCs are OCONUS (Korea and Germany), and approximately 560 PCs are located at the different sites across the CONUS. DMDC's goal is to refresh approximately one fifth of its PCs annually.

The contractor shall conduct testing, implementation, and administration of OS patches and upgrades approved for use by the Government on all end-user devices. This includes the application of all required security patches, version upgrades, security lockdowns, and installation of approximately 60 new or upgraded applications per year to some or all users. Historically 75 percent of software is distributed remotely.

Additionally, in support of this task, the contractor shall perform the following activities.

a. Maintain the current baseline image and create additional standard images that can be utilized on multiple hardware platforms. Perform maintenance to the baseline image for OS and application updates to include security patches, hot fixes, application update and upgrades, and any additional enterprise software. Baseline images, both desktop and server images, shall be updated with the latest patches and security updates and approved by DMDC's Cybersecurity Division. DMDC currently supports two Windows 10 desktop images, Standard User and Developer.
b. Provide support for the administration of all physical and virtual workstations, mobile computing devices, peripheral devices, and end-user software applications which support on-site and telework workforces in both the classified and unclassified environments.
c. Resolve end-user incidents related to on-site software or hardware and fulfill approved end-user requests for software, hardware, or configuration changes in accordance with DMDC governance rules.
d. Plan, analyze, and resolve end-user incidents related to on-site software or hardware, remote access infrastructure, and mobile devices.
e. The contractor shall troubleshoot (at Tier II) end-user equipment ensuring a fully operational state.
f. The contractor shall perform preventative maintenance such as cabling integration with computer systems.
g. Develop a plan to distribute mobile devices to end users as needed and implement the Government-approved plan.
h. Plan, analyze, troubleshoot, integrate, install, test and validate, operate, maintain, train, document, and provide administration services for all desktop hardware and software systems.

C.5.5.3.2 SUBTASK 3.2 – PROVIDE AUDIO/VISUAL ADMINISTRATION

The contractor shall provide Audio Visual/Video Teleconference Support. DMDC supports various sites with VTC capabilities, including the DoD Center, Seaside, CA (includes one classified VTC), and the Mark Center, Alexandria, VA; between these two sites there are nine rooms with VTC capabilities. Additional VTC sites currently supported are Defense Manpower Data Center, Defense Civilian Personnel Advisory Service (DCPAS), in Alexandria, VA, as well as DMDC, San Antonio, TX.

The contractor shall troubleshoot (at Tier II) VTC equipment ensuring, audio and video integration are in a fully operational state. The contractor shall perform preventative maintenance such as replacing lamp bulbs, cleaning filters, and cabling integration with computer systems.

Additionally, in support of this task, the contractor shall perform the following activities:

a. Maintain internal connectivity for NIPRNET and SIPRNET VTC connections within the DMDC Enterprise via switches, routers and firewalls, and other controlling factors.
b. Provide Tier I and Tier II support for Town Halls and other high-level meetings, including using DISA's Defense Collaboration Services (DCS) and the VTC.
c. Provide Tier I and Tier II troubleshooting and document all VTC support incidents; if it cannot be resolved at Tier II, then it is escalated to the vendor for Tier III support.

C.5.6 TASK 6 – TRANSFORMATIONAL IT SUPPORT

Transformational IT support is composed of support to maintain DMDC's testing laboratory and IT environments, to include development, pre-production (i.e., testing). This task also supports architecture analysis and the evaluation of emerging technologies that impact DMDC and its stakeholders. This task also includes supporting the maintenance of a SIPRNET presence through an Installation Processing Node (IPN) for Seaside and the Mark Center.

C.5.6.1 SUBTASK 6.1 – PROVIDE SYSTEMS ENVIRONMENTS FOR DEVELOPMENT, TESTING, AND PRE-PRODUCTION

The contractor shall provide a computer lab and agency-wide integration and testing environments, capable of supporting a myriad of IT systems, projects, and environments (physical and virtual) through their planning, development, testing, quality assurance, and deployment phases.

C.5.6.1.1 SUBTASK 1.1 – LAB SUPPORT

The contractor shall support and maintain a physical on-site lab at DMDC. The lab shall be scalable and connected to DMDC's visitor network (i.e., the internet). The contractor shall perform the following activities:

a. Schedule, coordinate, and plan use of lab resources.
b. Process, maintain, and file lab requests.
c. Provision and maintain equipment to include software for the effective functioning of the lab environment.
d. Maintain lab transaction reports, policies, and SOPs (Section F, Deliverable 20); process lab requests.
e. Perform system administration activities to support lab activities.
f. At the end of each test, breakdown and reset the lab to its baseline configuration.

The contractor shall maintain the lab during DMDC core hours. Hours outside of core hours will be approved by the FEDSIM COR or DMDC TPOC in the event that unscheduled access is required.

C.5.6.1.2 SUBTASK 1.2 – INTEGRATION AND TESTING ENVIRONMENTS

The contractor shall assist with the consolidation, modernization, and daily operation of DMDC's integration and testing environments. Currently, DMDC maintains multiple development and pre-production environments: test, model, demo, gold, silver, and stress test. The contractor shall provide support on the following:

a. Workstation (desktop, laptop, tablet, smartphone) analysis, administration, testing, and security.
b. Server (physical/virtual) analysis, administration, testing, and security.
c. Network (wired/wireless) architecture analysis, administration, testing, and security.
d. COTS/GOTS-approved software analysis, administration, testing, and security, to include deployment capabilities.
e. VOIP technologies analysis, administration, testing, and security.
f. Other new technologies.

Additionally, the contractor shall:

a. Propose methods or architectures allowing DMDC-specified test environments to communicate with needed production IT services while posing a manageable technical and security risk to the production environment (Section F, Deliverable 56).
b. Prepare and exercise testing scenarios to verify the operations stability of new hardware and software prior to its use.
c. Maintain operational status of the test environment.
d. Maintain and update test environment architecture and configuration settings to mirror the production environment.

As DMDC applications are migrated, the nature of integration and testing environments evolve; the contractor shall maintain these environments, providing support as data centers transition to their final states. As DMDC proceeds with migrating its applications, the contractor shall make recommendations to the Government on how to decrease the number of test environments that are permanently maintained through the use of cloud technology, virtualized environment, and plug-able database technology (Section F, Deliverable 56). Once approved by the Government, these recommendations shall be implemented.

The contractor shall support these environments from 4 AM Pacific Time (PT) through 8 PM PT Monday – Friday, and on Saturday 4 AM PT through 6 PM PT, with the availability of the environment meeting the levels provided in the PRS.

C.5.6.2 SUBTASK 6.2 – PROVIDE ARCHITECTURE ANALYSIS AND TECHNOLOGY EVALUATION SUPPORT

DMDC’s rapidly evolving business and mission environment demands innovative and efficient ways to provide properly secured access through shared critical business and mission-related information; response to the surging and receding mission needs; unpredictable service and changing support staffing needs; an ability to leverage existing information assets to meet emerging mission challenges; and the ability to optimize the benefits of IT applications expenditures.

The contractor shall recommend and suggest improvements which optimize performance, eliminate single points of failure, and enhance viability of DMDC Enterprise to support its growing base of customers (Section F, Deliverable 56).

The contractor shall perform systems and technology analysis to include the following:

a. New technology impact to DMDC (technology refresh).
b. Causal analysis and defect prevention.

c. Project planning for the implementation of technical solutions.
d. Technical requirements analysis and design.
e. System performance analysis across the enterprise DMDC, to include monthly reviews.
f. Trade studies and white papers on new technology to include cost analysis and recommendations.
g. Gap analysis.
h. Conducting feasibility studies for the implementation of new technologies.
i. Identification of possible product and software tool enhancement opportunities for improved performance and potential cost savings.

The contractor shall perform system modeling and simulation, testing, and prototyping to evaluate technology enhancements, providing recommendations on technical implementations, products and COTS evaluation, lifecycle planning, and technology enhancements.

C.5.6.3 SUBTASK 6.3 – SUPPORT SIPRNET PRESENCE

The SIPRNET presence shall support interconnectivity and global accessibility delivering services to all authorized users in these locations. The contractor shall support all required STIG and security controls monitoring to maintain applicable certifications and compliance with DoD policies is required at an acceptable level of risk of the certifier.

As migration activities commence, the Seaside, CA, server presence will be shrunk down to serve as an IPN. This IPN will provide authorized SIPRNET users access to the SIPRNET and DMDC’s applications and also support DMDC’s privileged users’ access to DISA’s Out Of Band (OOB) Network to allow software installs and application upgrades to be completed. The contractor shall then be responsible for maintaining DMDC’s SIPRNET IPN and associated LAN to the same level of support as required on the NIPRNET.

The contractor shall support a SIPRNET access presence both in Seaside, CA, as well as the Mark Center in Alexandria, VA, through the support and management of IPNs. The contractor shall ensure authorized users still have access to the SIPRNET for SIPRNET email access, general SIPRNET access, and privileged users can apply software patches and upgrades and make application changes as required. The IPN is a fixed center serving each of these locations that are not provided by the core SIPRNET centers in Columbus/Ogden. The contractor shall supply technical expertise and staff with the applicable security clearance level to maintain each IPN, to include FOC, desktop support, helpdesk support, SIPRNET access, security patching, server maintenance, access to DISA’s Cross Domain Solution (CDS), capacity management, and all of the other functions that are required to maintain a functional IPN.

C.5.7 TASK 7 – APPLICATION MIGRATION SUPPORT

This task provides the full range of application migration support to include the planning, analysis, execution, and decommissioning of DMDC’s application migration. This includes consolidation of ~15 DMDC data centers to two for SIPRNET and NIPRNET, a primary and a failover for each, and the maintenance of a SIPRNET presence through an IPN for the Seaside and Mark Center locations.

In accordance with the Federal Data Center Optimization Initiative (DCOI) established in the Office of Management and Budget (OMB) Memorandum M-16-19, DMDC is implementing a strategy to consolidate its applications into a more efficient cloud-based infrastructure. Over the next five years, DMDC will migrate over 500 applications currently residing in 15 locations. These applications vary in size and complexity. Of the data centers which have been identified as hosting applications to be migrated six are classified as large, four as medium, and five as small.

DMDC hosts applications on both the SIPRNET and NIPRNET, with extensive stores of highly sensitive Personally Identifiable Information (PII) on both networks. Depending on the network on which an application is hosted, DMDC will migrate SIPRNET application onto DISA's Standard Hosting Option and NIPRNET applications into a Software Defined Data Center (SDDC) using DISA's Capacity Services Hosting Option (CSHO). The contractor shall provide DMDC support for application migration for both DMDC's SIPRNET and NIPRNET environments.

C.5.7.1 SUBTASK 1 – PROVIDE SIPRNET MIGRATION SUPPORT (OPTIONAL SUBTASK)

The contractor shall support the migration of approximately 12 applications including databases which it will be migrating from the Seaside, CA, and Cheyenne Mountain, CO, and SIPRNET data centers to DISA-provided centers at Columbus, OH, and Ogden, UT. DMDC has established a Memorandum of Understanding (MOU) with DISA to migrate these applications to DISA. For the SIPRNET migration, the Government has selected a Standard Hosting Option arrangement with DISA. Under this Standard Hosting Option, DISA furnishes all Operating Environments (OEs) using service provider standard OE and common infrastructure. The storage amounts and type(s) allocated to each OE identified will satisfy DMDC's storage requirements and identifies the total storage required, to include the OS. Standard backup and recovery procedures have been set and agreed to between DMDC and DISA and will adequately meet the DMDC's backup and recovery needs. All ports and protocols required to support the DMDC's environment are compliant with DoD and DISA standards for both internal and external traffic.

The contractor shall support these application migrations, utilizing industry best practices in compliance with DoD policies and procedures governing SIPRNET environments. The contractor shall provide expert knowledge in database management, virtualization, and administration, as well as COOP planning for the SIPRNET migration.

Upon completion of the application migrations, the contractor shall perform a phased close-down, dispositioning appropriate equipment disposal of the equipment currently located in Cheyenne, CO, and any equipment no longer required in Seaside, CA, in accordance with all asset and property management policies. DMDC's strategy requires migration of all 12 applications and phased close-down within six months of Optional Subtask award.

The contractor shall support data center closure activities for DMDC's presence at the Cheyenne Mountain SIPRNET site and downsizing of the Seaside SIPRNET site to include decommission of hardware/software, ensuring that all storage devices decommissioned are wiped clean or destroyed (in accordance with agency procedures and Government-wide regulations) to avoid creating any security risk or data disclosure.

Decommissioning shall be in accordance with the following NIST standards:

a. FIPS 199 - “Standards for Security Categorization of Federal Information and Information Systems”
b. FIPS 200 - “Minimum Security Requirements for Federal Information and Information Systems”
c. NIST SP 800-53 - “Security and Privacy Controls for Federal Information Systems and Organizations”
d. NIST SP 800-64 - “Security Considerations in the System Development Life Cycle”
e. NIST SP 800-88 - “Guidelines for Media Sanitization”
f. NIST SP 800-171 - “Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations”

The contractor shall conduct an inventory of all equipment, including the ownership type (e.g., leased, rented, contractor-owned, or Government-owned) by data center (Section F, Deliverable 57). All leased, rented, or borrowed equipment shall be returned to the owners with appropriate coordination. All of the spare Government-owned equipment such as racks and furniture shall be dispositioned in accordance with DMDC and DMRO processes. The contractor shall support Government updates of all property and asset management systems accordingly.

C.5.7.2 SUBTASK 2 – DEVELOP SIPRNET IPN CAPABILITY – SEASIDE (OPTIONAL SUBTASK)

The contractor shall build out an IPN for SIPRNET access which will be sustained by the contractor. This support shall be provided in the base period upon completion of Subtask C.5.7.1 and is anticipated to be completed in the Base Period. The contractor shall provide support to develop and deliver an IPN access capability at the DMDC Seaside location. The contractor shall supply technical expertise and staff with the appropriate security clearance level to support developing the infrastructure and capability to operate an IPN at the Seaside location. (Section F, Deliverable 57). This includes all applicable expertise to ensure compliance with all DoD security protocols.

C.5.7.3 SUBTASK 3 – DEVELOP SIPRNET IPN CAPABILITY - MARK CENTER (OPTIONAL SUBTASK)

The contractor shall build out an IPN for SIPRNET access which will be sustained by the contractor. This support shall be provided in the base period upon completion of Subtask C.5.7.1 and is anticipated to be completed in the Base Period The contractor shall provide support to develop and deliver an IPN access capability at the DMDC Mark Center location. The contractor shall supply technical expertise and staff with the appropriate security clearance level to support building the infrastructure and capability to operate an IPN at the Mark Center location (Section F, Deliverable 58). This includes all applicable expertise to ensure compliance with all DoD security protocols.

C.5.7.4 SUBTASK 4 – SUPPORT NIPRNET APPLICATION MIGRATION

DMDC has identified approximately 500 applications, including databases, which currently reside within various data centers on the NIPRNET. DMDC intends to migrate these applications from the various data centers over the course of this TO. As migrations commences, reference NIPRNET Migration Draft Schedule in the Electronic Reading Room. During migration additional support to other task activities, to include helpdesk, server administration, etc., will increase in order to effectively support users and systems which are currently provided by commercially hosted applications support. DMDC has determined its strategy for this move and is working with another Government agency to build out capacity at DISA in anticipation of the first migrations. The service model selected for hosting these applications will be referred to as a Capacity Services Hardware Option (CSHO), a private virtual cloud in an SDDC. During this migration, the Government will identify the applications which the contractor shall be responsible for supporting at an availability level of 99.99 percent.

Under this construct, the DISA will supply the hardware (servers, routers, etc.), racks, floor space, “pipe, power, and light” (e.g., power, NIPRNET access, air conditioning, backup power supply, and generators), and physical security. DMDC will supply all software licenses. DISA will also acquire and physically install and connect all racks, servers, storage, and network communications equipment identified in DMDC’s Bill of Materials documents. DISA will provide a floor plan based on power and Heating, Ventilation, and Air Conditioning (HVAC) requirements. DMDC will acquire and supply all required COTS software. The initial buildout of this DDC is being performed outside the scope of this contract and should be underway at the time of TO award. The contractor shall engage in observing, assisting, and learning the details of this buildout, as upon completion of the buildout, the contractor shall be responsible for its support, maintenance, and configuration from the OS up. The contractor shall also be responsible for implementing any subsequent growth as additional applications migrating in require increased capacity.

Specifically, the contractor shall

a. Install, configure, STIG, patch, administer, and monitor DMDC-furnished software.
b. Configure, STIG, patch, administer, monitor, and manage all network communications equipment connected to DMDC’s network.
c. Configure, administer, monitor, patch, and manage the storage solution.
d. Manage backup and recovery services.
e. Provide IA management, application administration, system administration, database administration, and service desk and infrastructure support to include reporting and coordinating hardware maintenance and repair with DISA.

DMDC, in coordination with the contractor, is responsible for COOP planning, testing, and audit response. DMDC will provide the detailed network design with cable plan. DMDC will also provide the detailed system design and rack elevations. The contractor, on behalf of DMDC, is solely responsible for the accreditation and security boundary counter defenses of the DMDC enclave and for obtaining and maintaining a security accreditation ATO on these environments.

The SDDC is a totally virtualized environment based heavily around the use of VMWare products and RedHat and includes the use of multiple automation tools. The contractor shall maintain the environment and expand its capability, as well as provide technical assistance to

DMDC in order to migrate multiple applications into this environment. The contractor shall also establish the appropriate level of DR for each application migrating to the environment.

DMDC has established an inventory of applications at its various data centers and is establishing an application migration plan to be implemented by the contactor. Application migrations considerations will be based on application and database dependencies as well as the current location of the application(s). Each group of NIPRNET application migrations will go through a discovery phase, a planning and analysis phase, an execution phase, and a closeout phase. Application migrations will occur at varying levels of complexity during the life of this TO.

C.5.7.4.1 SUBTASK 4.1 – PROVIDE DETAILED DISCOVERY IN SUPPORT OF APPLICATION MIGRATION

The contractor shall support detailed discovery in order to refine and verify the migration strategies and optimization plan, utilizing best business practices and additional server and application data. The contractor shall deliver a detailed Center Discovery Report for each center prior to migration (Section F, Deliverable 59). In support of detailed discovery, the contractor shall support the following:

a. Conduct data verification workshops.
b. Obtain additional detailed server and applications information, to include any unique hardware and software requirements.
c. Obtain applicable specific SOPs, TTPs, and other relevant documentation.
d. Review SLAs (e.g., uptime, availability, etc.,) with providers to ensure bilateral understanding and agreement.
e. Verify infrastructure requirements and plans.
f. Provide a Center Discovery Report.

C.5.7.4.2 SUBTASK 4.2 – PROVIDE ANALYSIS AND PLANNING FOR APPLICATION MIGRATION

The contractor shall utilize the inputs of the detailed discovery phase to develop and maintain an Application Migration Plan for each group of applications being migrated (Section F, Deliverable 59). Whenever possible, the initial migration shall be to move the application(s) into the new development environment to ensure and address any compatibility issues with operating in a totally virtualized environment. Any application coding changes required to run in the virtual environment are outside the scope of this contract and will be the responsibility of the application owner. Upon successful execution of the application in development, the application shall then migrate into pre-production to allow any required external connections to be tested, as well as to allow external users to exercise the application. Any environment changes required in development and pre-production shall be documented in DMDC's Change Management Database and also reflected in DMDC's production environment (where applicable) to ensure a smooth migration to production and that these environments are kept in sync. Upon success in pre-production, the application shall be migrated into DMDC's new production environment.

The purpose of this step is to complete and baseline the hour-by-hour plan that will be used during production cutover as well as preparing the receiving environment. The Plan shall contain and address the following activities.

a. Identify and document application maintenance responsibilities and access schedules.
b. Identify and document application maintenance responsibilities for patch management.
c. Obtain RMF paperwork to reflect the current application and hosting environment.
d. Analyze cyber security impacts of a transition to a new data center to ensure that all security requirements will be met in the new environment, and if changes are required to do so, the plan shall provide options on how to include those changes.
e. Facilitate project update meetings as directed by the Government to review the status of the WBS, risk register, and migration plan.
f. Develop a detailed WBS for each migration (Section F, Deliverable 59), a plan for Synchronization Meetings (Section F, Deliverable 59), and a Risk Register (Section F, Deliverable 28) (e.g., detailed schedule phased move event and solutions incorporated into the transition plans).
g. Develop the implementation plan to achieve the Government-defined migration strategy and create supporting architectural documentation, coordinating approvals.
h. Develop technical solution design and proof-of-concept approach for any application migration.
i. Assess available capacity of the destination data center to ensure current infrastructure can support the increased capacity required of the planned migration.
j. Identify any increased hardware capacity and additional software required to ensure capacity exists to support the planned migration of the targeted applications and data repositories.
k. Establish hardware specifications, acquisition, and logistical setup definitions for all new equipment (Section F, Deliverable 59) and provide to Government so DMDC can work this requirement with DISA.
l. Verify applications for compliance with all of the security and operations rules of the new hosting location (that may be enforced differently than the current hosting environment).
m. Address application integration planning.
n. Contain a data migration strategy to support the application migration to include all data repositories, ensuring no loss of currency in the data.
o. Baseline hour-by-hour plan.
p. Migration plan (to include the identification of any application "freeze" period that may be required).
q. Application test plan.
r. What measures will be used to determine "success."
s. Fallback plan.

The contractor shall ensure that all application freeze and transition periods are negotiated with the business system owner well in advance of the application migration to ensure program planning can accommodate or mitigate negative impacts.

The contractor shall collaborate on the integration of DMDC's detailed migration WBS in the overall Project Management Plan (Section F, Deliverable 9) to ensure all known dependencies, requirements, milestones, and tasks are identified and aligned in support of DMDC and their external partners.

C.5.7.4.3 SUBTASK 4.3 – CONDUCT APPLICATION MIGRATION EXECUTION

The contractor shall execute application migration in accordance with the Government-approved application migration plan and required uptime as dictated in the PRS, utilizing industry best practices based on applicability of the environment.

The contractor shall ensure that proposed migration groupings and schedules are submitted for final Government approval and the application project managers prior to execution (Section F, Deliverable 59). The contractor shall ensure that key stakeholders agree on the schedule with proper notification to the user community before applications are migrated, and that the helpdesk is notified in advance of any migrations that might impact the end-user's experience or application availability.

Until directed by the Government, the applications shall be maintained at both the legacy and new locations. The contractor shall work with application owners to validate that the applications function correctly in the preproduction environment and are then validated in the new production environment.

With the migration of each application group, the contractor shall update RMF-associated documentation to reflect any changes made to the new environment.

C.5.7.4.4 SUBTASK 4.4 – SUPPORT DATA CENTER CLOSURE ACTIVITIES

The contractor shall support data center closure activities for NIPRNET sites to include decommission of hardware/software, ensuring that all storage devices decommissioned are wiped clean or destroyed (in accordance with agency procedures and Government-wide regulations) to avoid creating any security risk or data disclosure.

Decommissioning shall be in accordance with the following NIST standards:

a. FIPS 199 - "Standards for Security Categorization of Federal Information and Information Systems"
b. FIPS 200 - "Minimum Security Requirements for Federal Information and Information Systems"
c. NIST SP 800-53 - "Security and Privacy Controls for Federal Information Systems and Organizations"
d. NIST SP 800-64 - "Security Considerations in the System Development Life Cycle"
e. NIST SP 800-88 - "Guidelines for Media Sanitization"
f. NIST SP 800-171 - "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations"

The contractor shall conduct an inventory of all equipment, including the ownership type (e.g., leased, rented, contractor-owned, or Government-owned) by data center (Section F, Deliverable 59). All leased, rented, or borrowed equipment shall be returned to the owners with appropriate coordination. All of the spare Government-owned equipment such as racks and furniture shall be dispositioned in accordance with DMDC and DMRO processes. The contractor shall support Government updates of all property and asset management systems accordingly.

C.5.8 TASK 8 – SURGE SUPPORT (OPTIONAL TASK)

As an agency of the DoD, DMDC must respond to real-world changes, whether it is a new reform initiative, top-down policies and mandates, or even national security interests and immediate threats. It is essential that DMDC have the IT resources and means to support evolving threats.

Projects include, short-term (less than 90 calendar days) response to implement directives, support to cybersecurity-related events, and helpdesk surge to support complex upgrades.

The contractor shall provide staffing resources within scope of the current TO to fulfill unplanned projects or unanticipated requirements. The contractor shall use industry best practices and subject matter expertise to execute additional, as–needed, related projects.

Surge support shall include, but is not limited to, the following activities:

a. Additional resources to support the relocation of IT infrastructure.
b. Rapid capabilities that mitigate or resolve major IT issues, cybersecurity threats, national security events, policy changes, and impacts.
c. Major system roll outs.
d. Implementation of new DoD programs.
e. Transition or transfer of existing DoD programs.

The contractor shall account for additional as-needed activities and provide the resources necessary to accommodate them. The resources may include an SME for program review, analysis, and integration strategies. During the life of the TO, the workload in any one area may grow significantly for a period of time. When a surge requirement is identified by the Government, the surge CLIN will be exercised. The CO or COR will provide the contractor with a requirements document specifying the surge requirement, and expected outcomes. The contractor shall develop a Surge Plan (Section F, Deliverable 60) which shall include, project approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government. The contractor shall staff surge resources within 30 calendar days of formal written approval of the Surge Plan. The Government shall use existing performance metrics and SLAs to measure surge-related performance.